DrayTek

Vigor2700Ge/e

ADSL2/2+ Firewall Router

User's Guide V1.0

DrayTek

Vigor 2700Ge/e
ADSL2/2+ Firewall Router
User's Guide

Version: 1.0

Date: 2005/11/14

Table of Contents

1 Preface

Targeting requirement for residential, SOHO (Small Office and Home Office) and business users, the Vigor2700Ge/e is an ADSL2/2+ enabled integrated access device. With downstream speed up to 12Mbps (ADSL2) or 24Mbps (ADSL2+), the Vigor2700Ge/e provides exceptional bandwidth for Internet access.

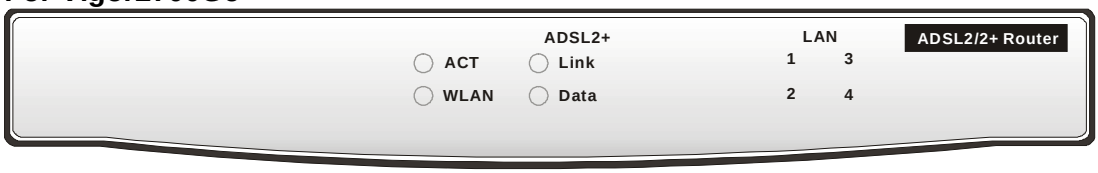
To secure your network, the Vigor2700Ge/e provides an advanced firewall with advanced features, such as Stateful Packet Inspection (SPI) to offer network reliability by detecting and prohibiting malicious penetrating packets or DoS attacks, user-configurable web filtering for parental control against network abuse etc.

Vigor 2700Ge is embedded with an 802.11g compliant wireless module which provides wireless LAN access with data rate as much as 54Mbps. As for data privacy of wireless network, the Vigor2700Ge can encode all transmissions data with standard WEP and industrial strength WPA2 (IEEE 802.11i) encryption. Additional features include Wireless Client List and MAC Address Control for maintaining control over user's authorization in your network, and Hidden SSID for being invisible to outside intruders scanning.

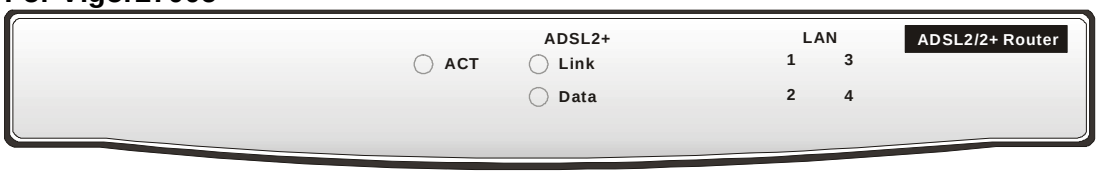
1.1 LED Indicators and Connectors

The displays of LED indicators and connectors for the routers are different slightly.

For Vigor2700Ge



For Vigor2700e



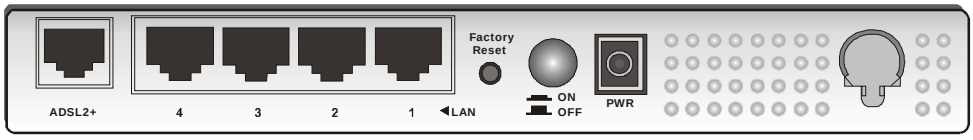
1.1.1 LED Explanation

LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	On	The router is powered on.
WLAN	Off	Wireless access point is turned off.
	On	Wireless access point is ready.
	Blinking	Wireless traffic goes through.
ADSL2+ Link	On	ADSL is show time.
	Blinking	The device starts handshaking.
ADSL2+ Data	Blinking	Data is transmitting.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

1.1.2 Connector Explanation

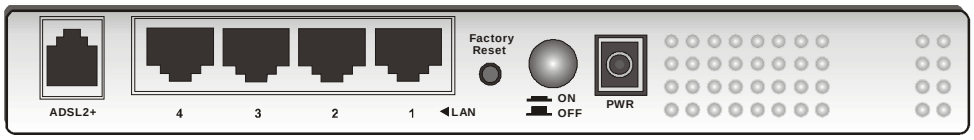
For Vigor2700Ge

for Annex A

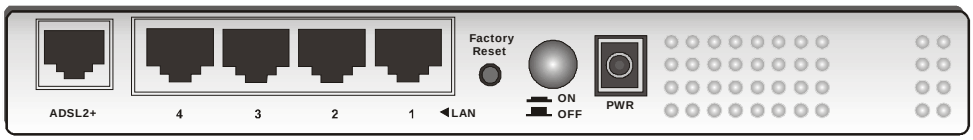


for Annex B

For Vigor2700e



for Annex A



for Annex B

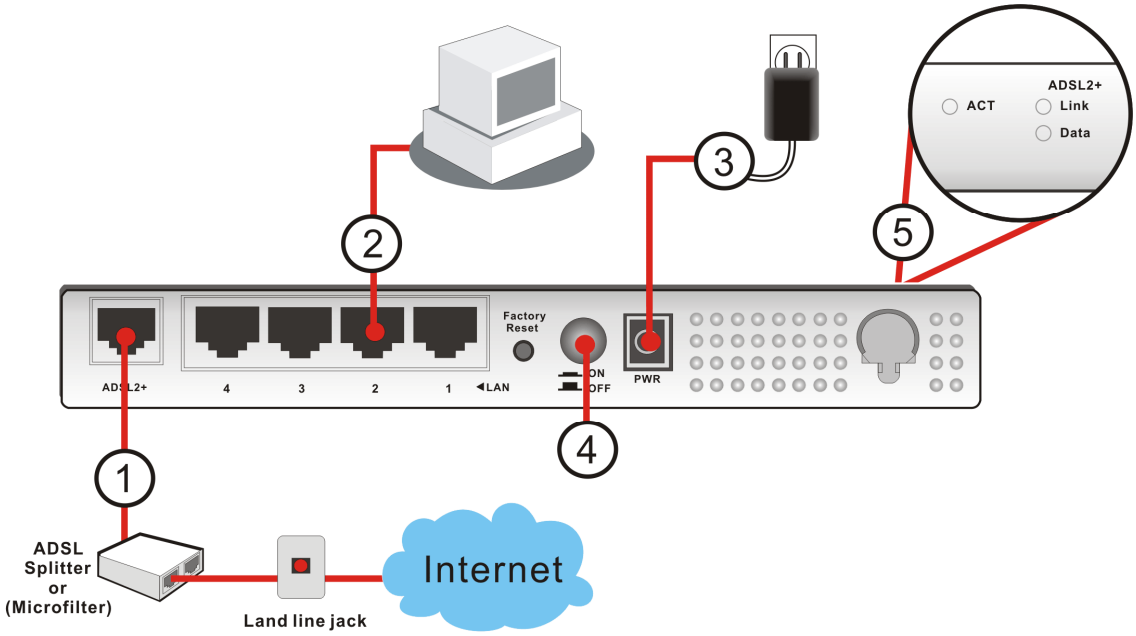
Interface	Description
ADSL 2+	Connecter for accessing the Internet through ADSL 2+.
LAN 4 – 1	Connecter for local networked devices.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
ON/OFF	Power Switch.
PWR	Connecter for a power adapter with 7~7.5VDC.

1.2 Hardware Installation

Before starting to configure the router, you have to connect your devices correctly.

1. Connect the DSL interface to the external ADSL splitter with an ADSL line cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the router.
5. Check the **ACT** and **ADSL2+**, **LAN** LEDs to assure network connections.

(For the detailed information of LED status, please refer to section 1.1.)


ADSL2+
ACT
Link
Data
5
3
2
Factory
Reset
ADSL2+
4
3
2
1
LAN
ON
OFF
PWR
4
1
ADSL
Splitter
or
(Microfilter)
Land line jack
Internet

2 Configuring Basic Settings

For use the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

This chapter explains how to setup a password for an administrator and how to adjust basic settings for accessing Internet successfully. Be aware that only the administrator can change the router configuration.

2.1 Changing Password

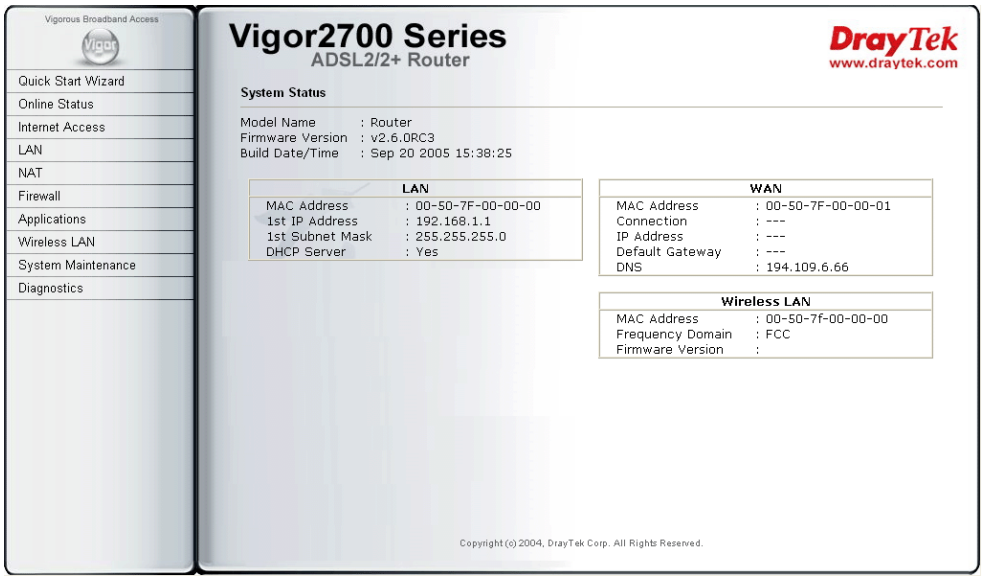
To change the password for this device, you have to access into the web browse with default password first.

1. Make sure your computer connects to the router correctly.

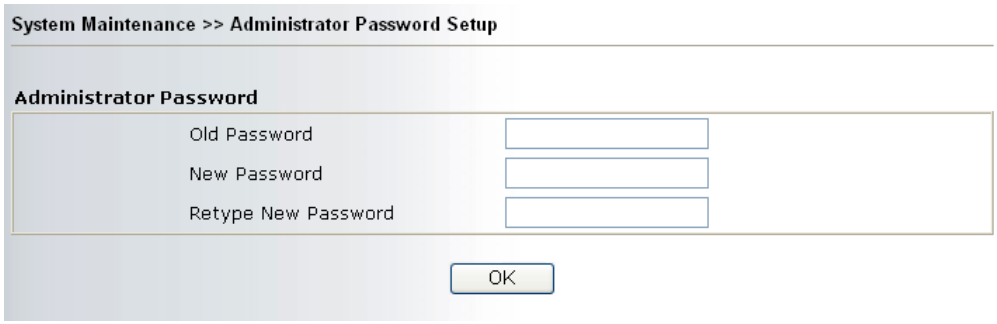
Notice: You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of this guide.

2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Please type default values (both username and password are Null) on the window for the first time accessing and click **OK** for next screen.

3. Now, the **Main Screen** will pop up.



4. Go to **System Maintenance** page and choose **Administrator Password**.

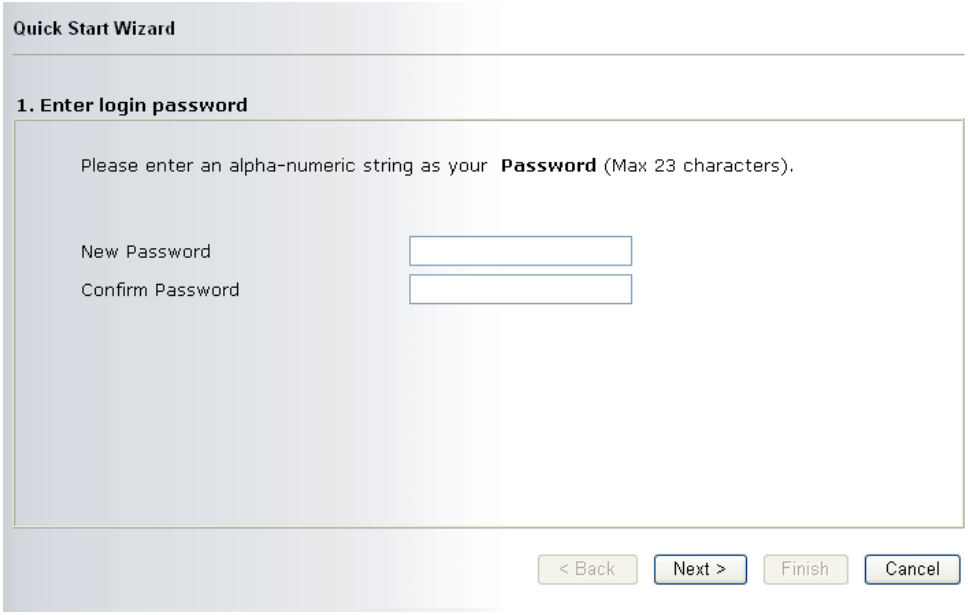


5. Enter the login password (the default is blank) on the field of **Old Password**. Type a new one in the field of **New Password** and retype it on the field of **Retype New Password**. Then click **OK** to continue.

6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

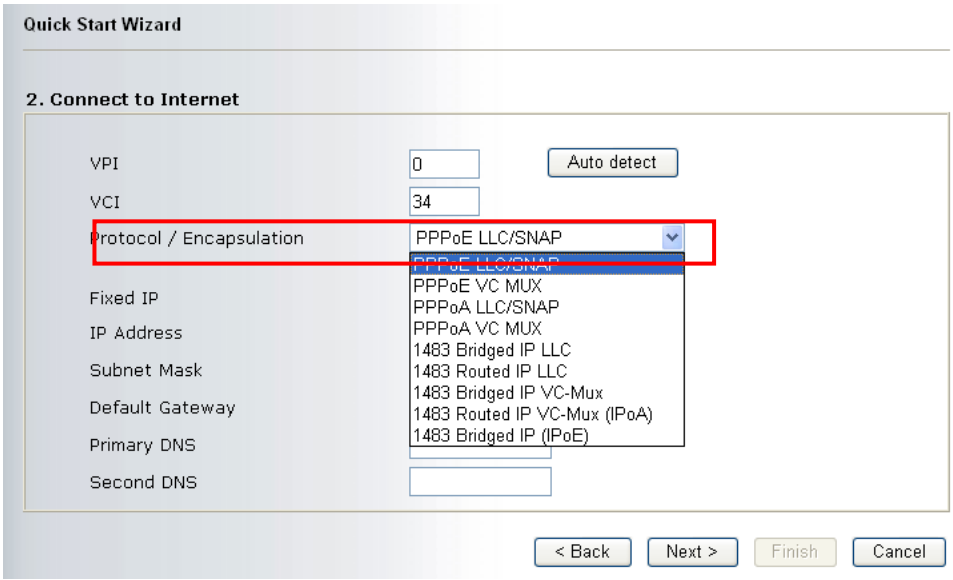
2.2 Quick Start Wizard

If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.



2.2.1 Adjusting Protocol/Encapsulation

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPPoA, Bridged IP, or Routed IP**. The router supports the Ethernet WAN interface for Internet access.



Now, you have to select an appropriate WAN connection type for connecting to the Internet through this router according to the settings that your ISP provided.

VPI Stands for **Virtual Path Identifier**. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.

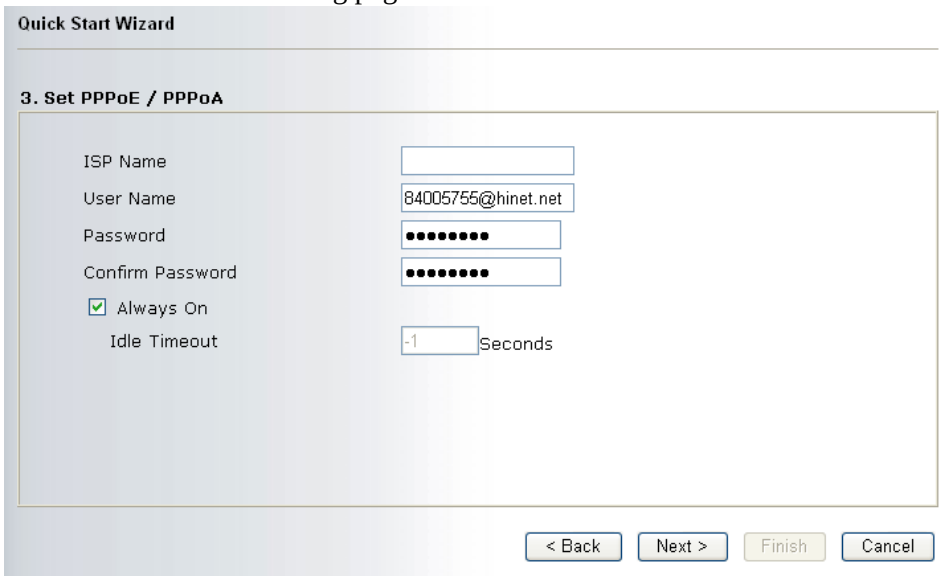
VCI	Stands for **Virtual Channel Identifier.** It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.
Protocol/Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA, Bridged IP** and **Routed IP**.
Fixed IP	Click **Yes** to specify a fixed IP for the router. Otherwise, click **No (Dynamic IP)** to allow the router choosing a dynamic IP. If you choose **No**, the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign a private IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of **Routed IP** and **Bridged IP**.
Default Gateway	Assign a private IP address to the gateway for the protocol of **Routed IP** and **Bridged IP**.
Primary DNS	Assign a private IP address to the primary DNS.
Second DNS	Assign a private IP address to the secondary DNS.

2.2.2 PPPoE/PPPoA

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection. And the PPPoA stands for Point-to-Point Protocol over ATM. PPPoA uses the PPP dial-up protocol with ATM as the transport.

PPPoE or PPPoA is used for most of DSL modem users. All local users can share one PPPoE or PPPoA connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

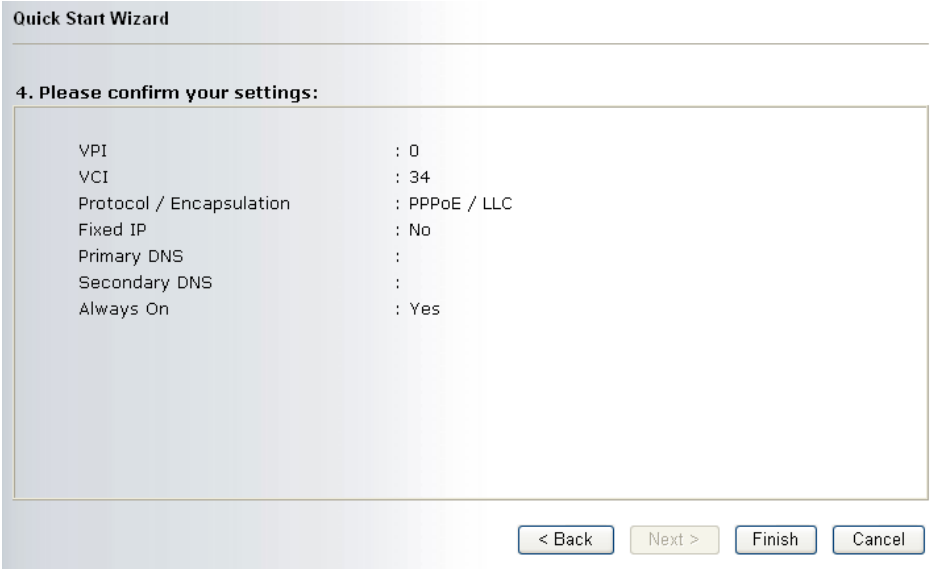
If your ISP provides you the **PPPoE** or **PPPoA** connection, please select **PPPoE** or **PPPoA** for this router. The following page will be shown:



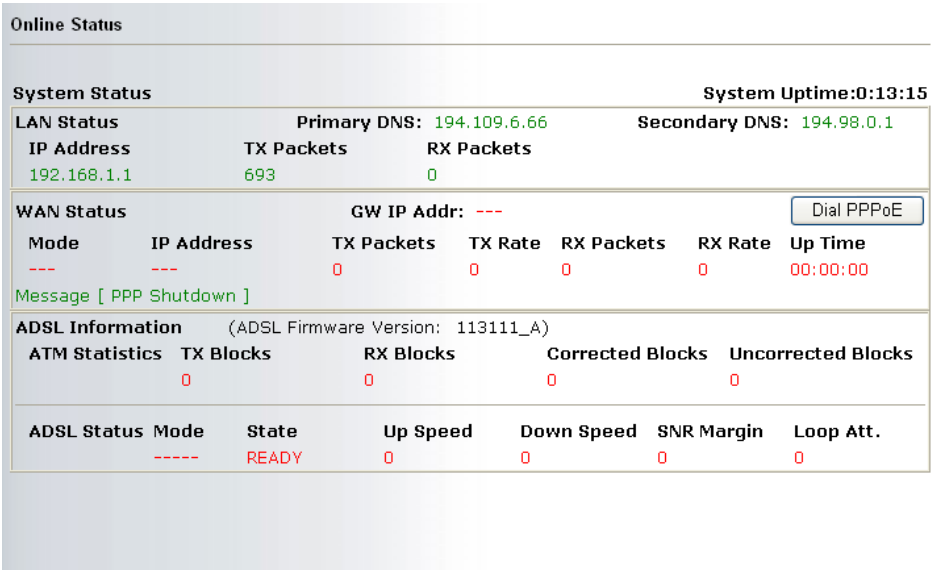
ISP Name	Assign a specific name for ISP requirement.

User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.
Always On	Check this box to allow the router connecting to Internet forever.
Idle Timeout	Type in the value (unit is second) as the idle timeout of the connection.

Click **Next** for viewing summary of such connection.

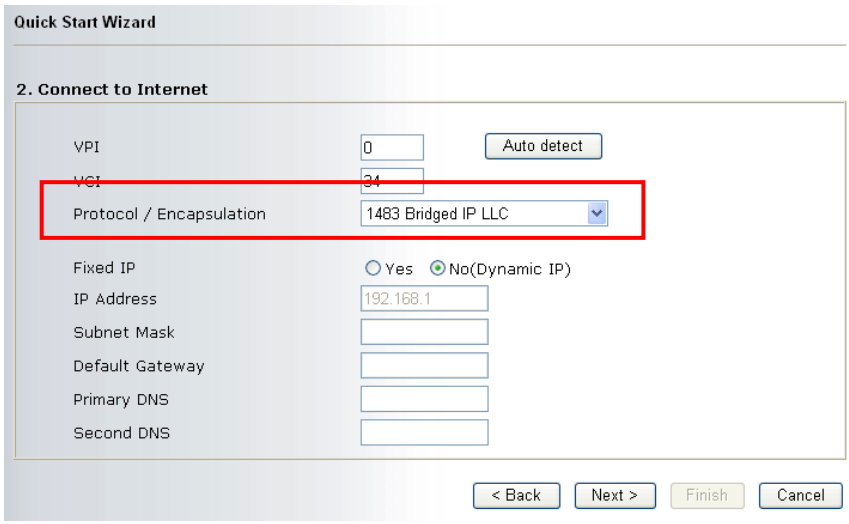


Click **Finish.** The online status of this protocol will be shown as below.

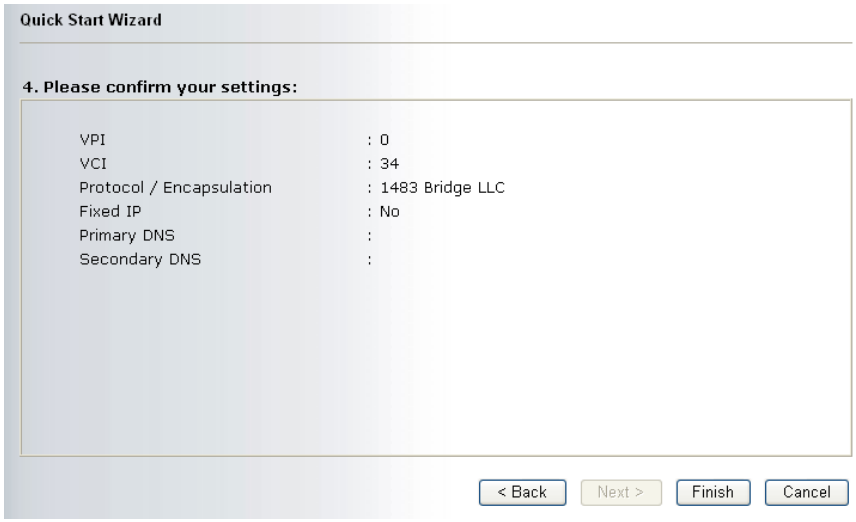


2.2.3 Bridged IP

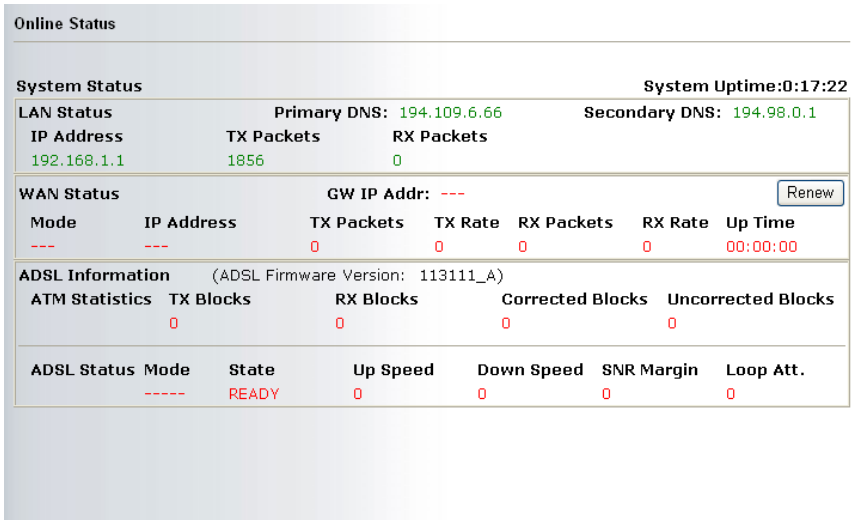
Click **1483 Bridged IP** as the protocol. Type in all the information that your ISP provides for this protocol.



After finishing the settings in this page, click **Next** to see the following page.

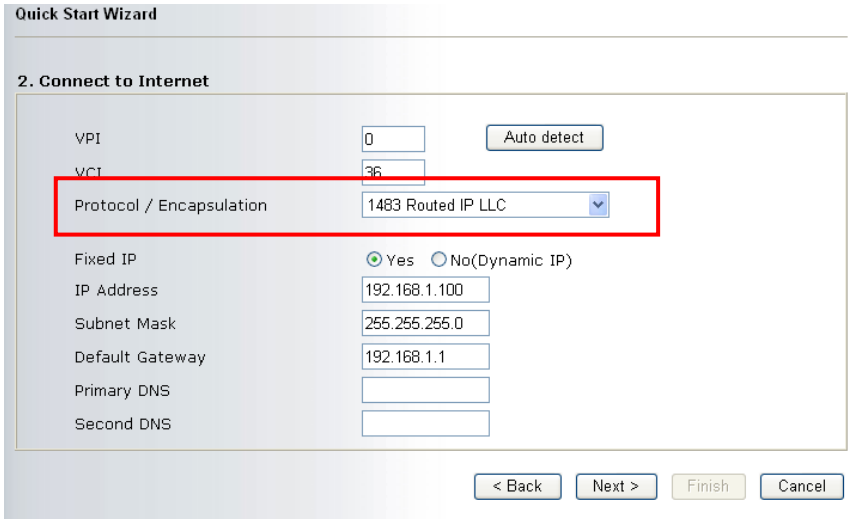


Click **Finish.** The online status of this protocol will be shown as below.

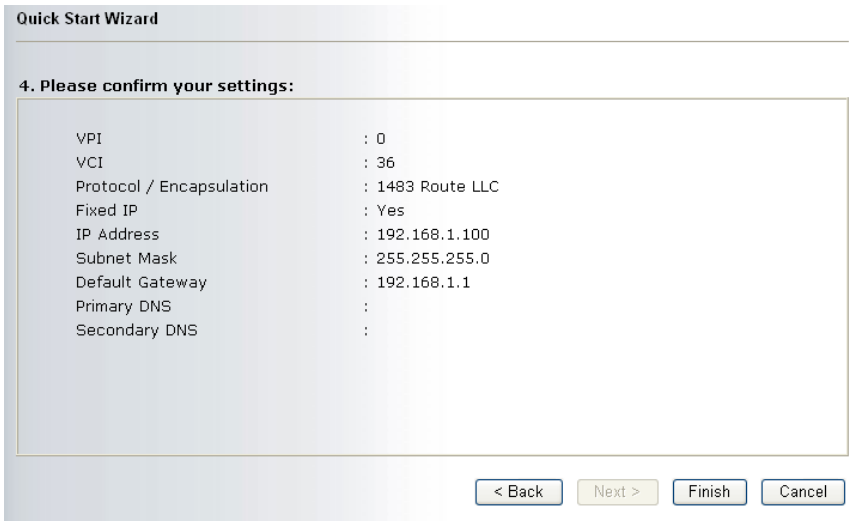


2.2.4 Routed IP

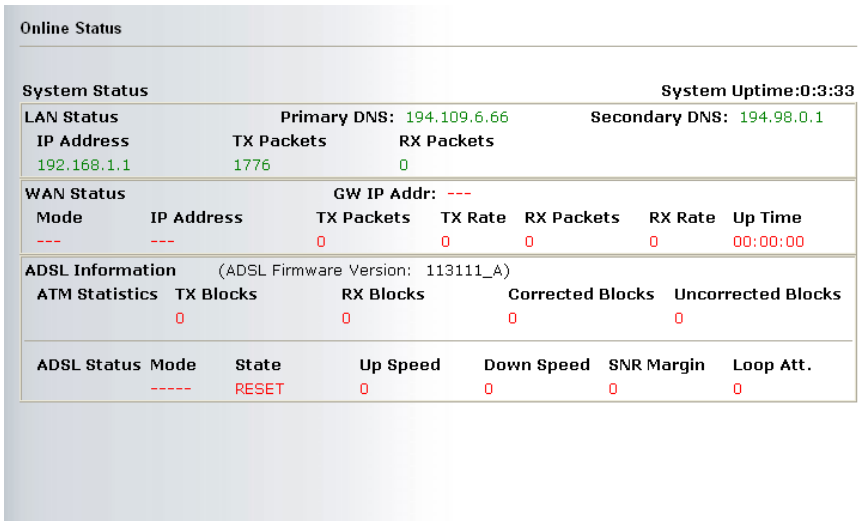
Click **1483 Routed IP** as the protocol. Type in all the information that your ISP provides for this protocol.



After finishing the settings in this page, click **Next** to see the following page.



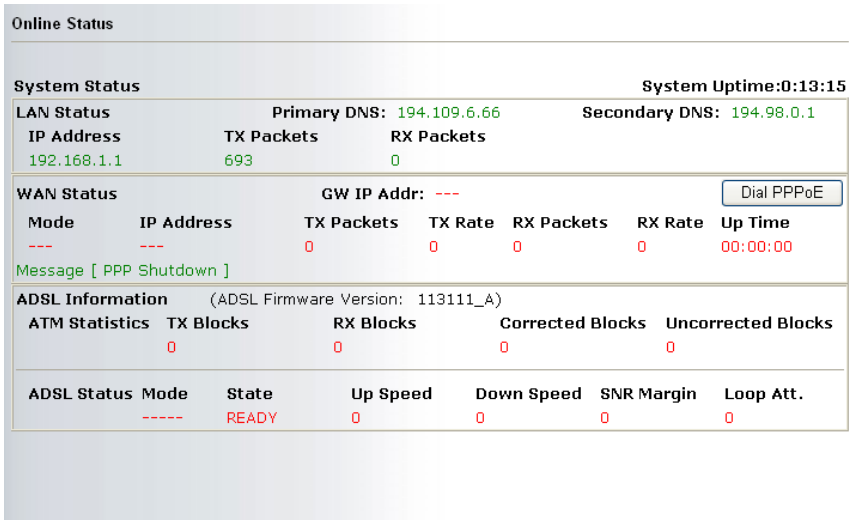
Click **Finish.** The online status of this protocol will be shown as below.



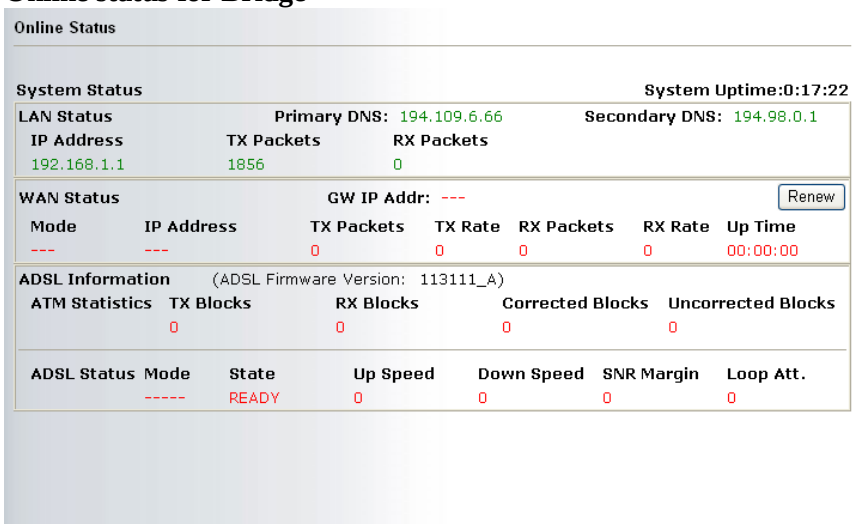
2.3 Online Status

The online status shows the system status, WAN status, ADSL Information and other status related to this router within one page. If you select **PPPoE** or **PPPoA** as the protocol, you will find out a button of **Dial PPPoE** or **Dial PPPoE** in the Online Status web page.

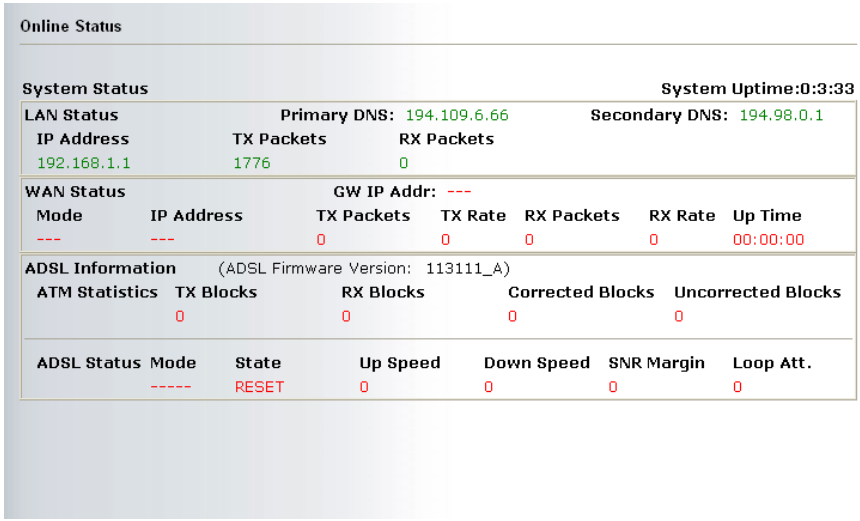
Online status for PPPoA/PPPoE



Online status for Bridge



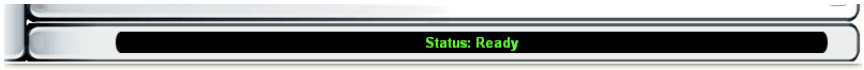
Online status for Routed IP



Primary DNS	Displays the assigned IP address of the primary DNS.
Secondary DNS	Displays the assigned IP address of the secondary DNS.
IP Address (in LAN)	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
GW IP Addr:	Displays the assigned IP address of the default gateway.
IP Address (in WAN)	Displays the IP address of the WAN interface.
TX Rate	Displays the speed of transmitted packets at the WAN interface.
RX Rate	Displays the speed of received packets at the WAN interface.
Up Time	Displays the total system uptime of the interface.
ADSL Information	Displays the firmware version of this router.

2.4 Saving Configuration

Each time you click **OK** on the web page for saving the configuration, you can find messages showing the system interaction with you.



Ready indicates the system is ready for you to input settings.

Settings Saved means your settings are saved once you click **Finish** or **OK** button.

3 Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more settings for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to Chapter 4.

3.1 Internet Access

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as ***private*** IP addresses, and are listed in the following ranges:

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all of the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

To acquire a public IP address from your ISP for Vigor router as a customer premises equipment, there are three common protocols: Point to Point Protocol over Ethernet (**PPPoE), PPPoA and MPoA**. **Multi-PVC** is provided for more advanced setup of the above.

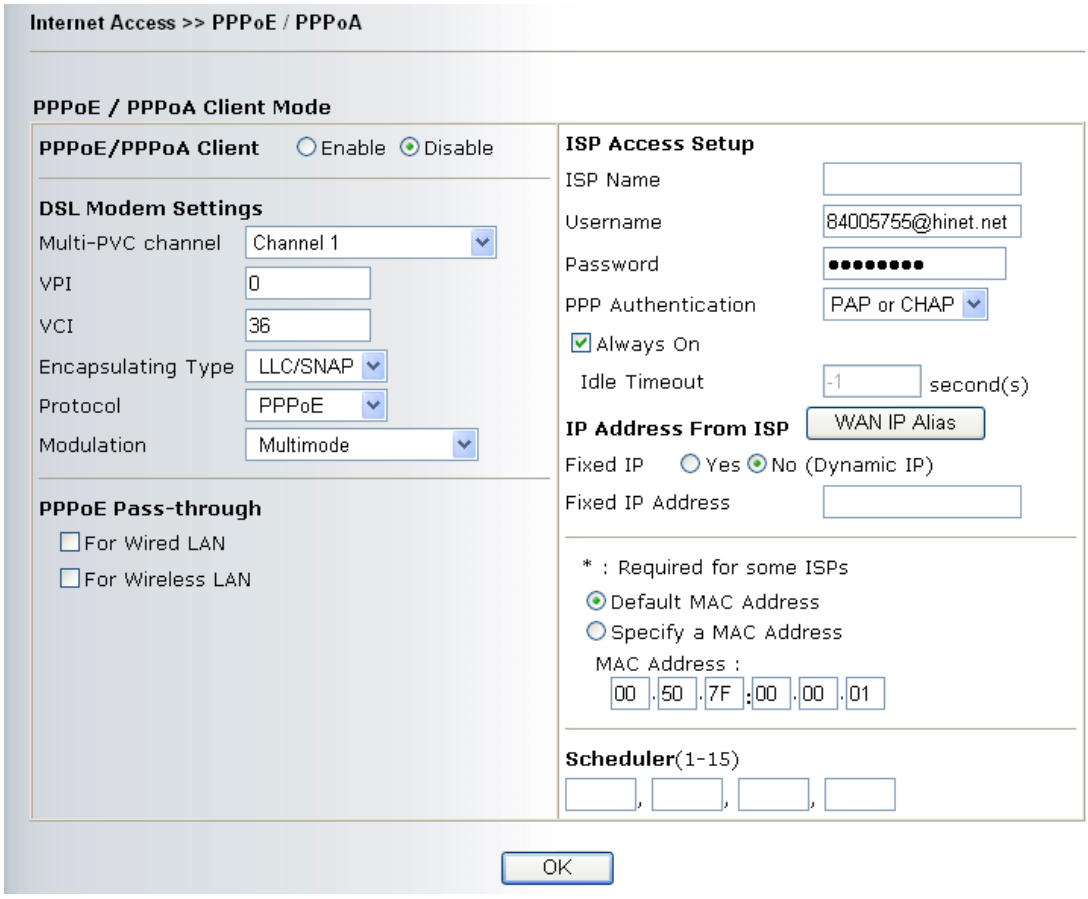
In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

3.1.2 PPPoE/PPPoA

PPPoA, included in RFC1483, can be operated in either Logical Link Control-Subnetwork Access Protocol or VC-Mux mode. As a CPE device, Vigor router encapsulates the PPP session based for transport across the ADSL loop and your ISP's Digital Subscriber Line Access Pultiplexer (SDLAM).

To choose PPPoE or PPPoA as the accessing protocol of the internet, please select **PPPoE/PPPoA** from the **Internet Access** menu. The following web page will be shown.



PPPoE/PPPoA Client Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

DSL Modem Settings Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
Multi-PVC channel – The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be chosen.
VPI - Type in the value provided by ISP.
VCI - Type in the value provided by ISP.
Encapsulating Type - Drop down the list to choose the type provided by ISP.
Protocol - Drop down the list to choose the one provided by ISP.
If you have already used **Quick Start Wizard** to set the protocol, then it is not necessary for you to change any settings in this group.

PPPoE Pass-through The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router.

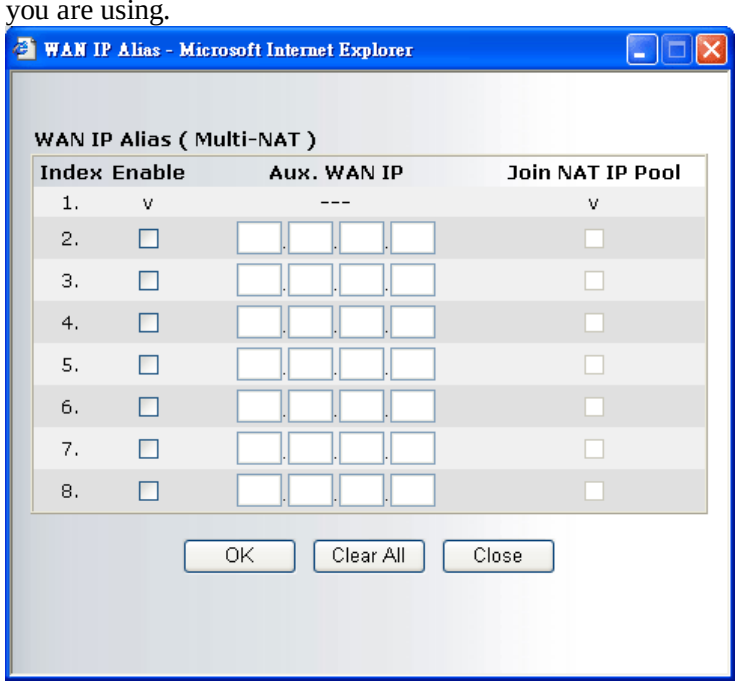
For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.
For Wireless LAN – If you check this box, PCs on the same network through wireless connection can use another set of PPPoE session (different with the Host PC) to access into Internet.

ISP Access Setup

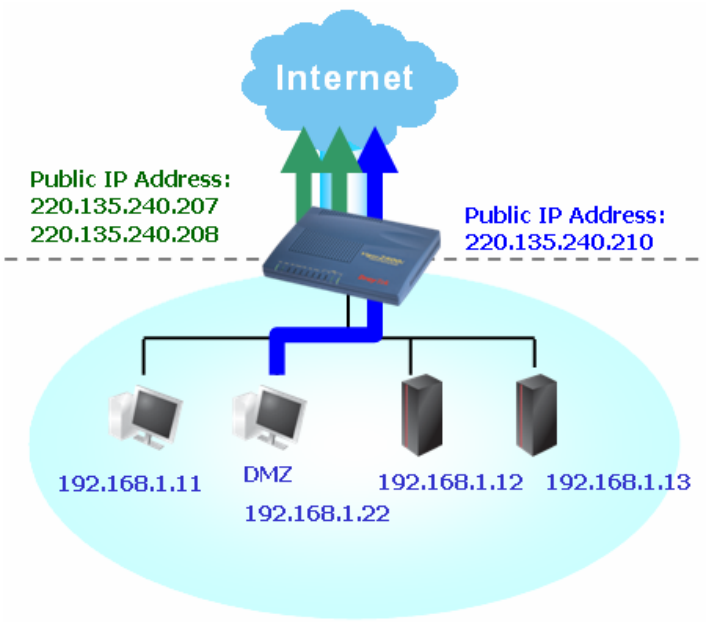
Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.
ISP Name – Type in the ISP Name provided by ISP in this field.
Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
PPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.
Always On – Check this box if you want the router keeping connecting to Internet forever.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.

IP Address From ISP

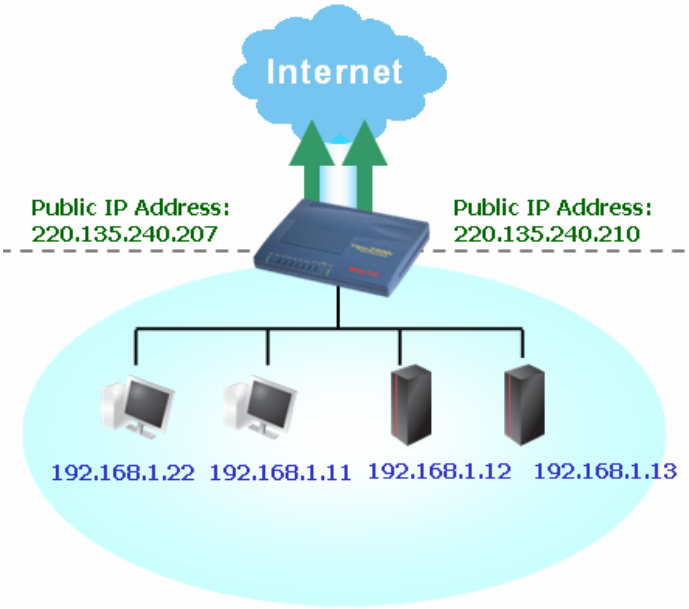
Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.
Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box.
WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.



By checking the checkbox **Join NAT IP Pool**, data from NAT hosts will be round-robin forwarded on a session basis.



If you do not check **Join NAT IP Pool**, you can still use these public IP addresses for other purpose, such as DMZ host, Open Ports.



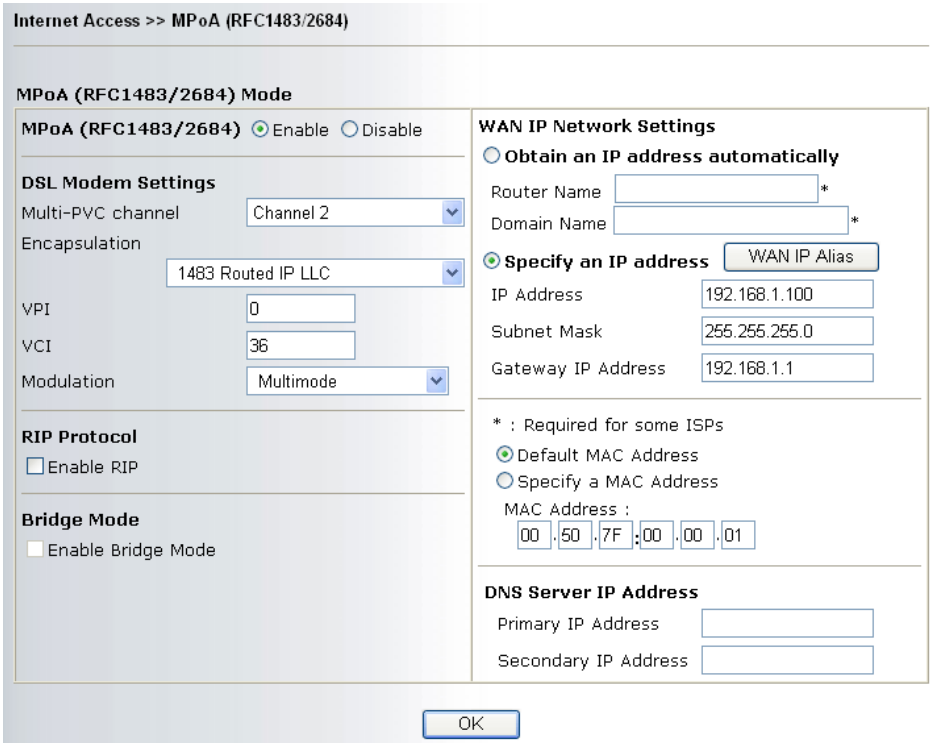
Default MAC Address	Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity. MAC Address – Type in the MAC address for the router manually.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

After finishing all the settings here, please click **OK** to activate them.

3.1.3 MPoA

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, token-ring or TCP/IP protocols. The goal of MPoA is to allow different LANs to send packets to each other via an ATM backbone.

To choose **MPoA** as the accessing protocol of the internet, please select **MPoA** from the **Internet Access** menu. The following web page will be shown.



MPoA (RFC1483/2684) Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

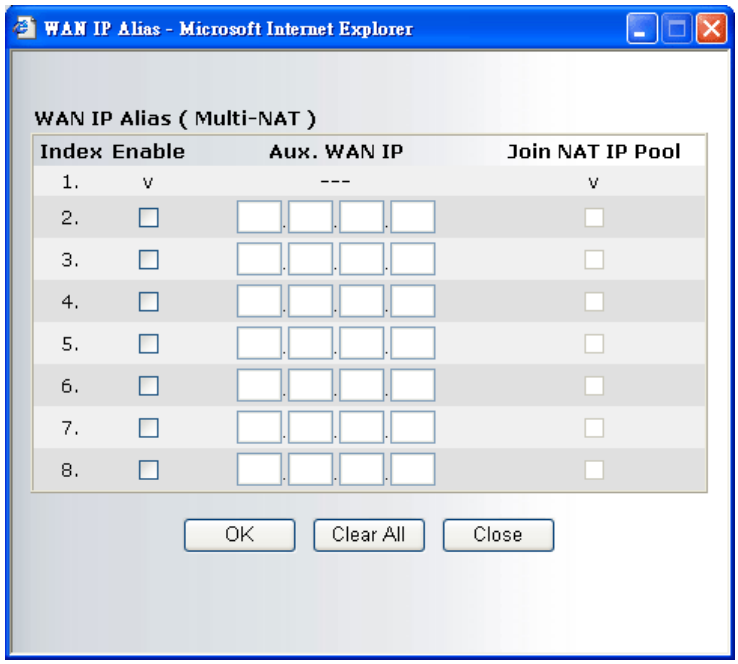
DSL Modem Settings Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
Multi-PVC channel - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be chosen.
Encapsulating Type - Drop down the list to choose the type provided by ISP.
VPI - Type in the value provided by ISP.
VCI - Type in the value provided by ISP.

RIP Protocol Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.

Bridge Mode If you choose **Bridged IP** as the protocol, you can check this box to invoke the function.

WAN IP Network Settings This group allows you to obtain an IP address automatically and allows you type in IP address manually.

Obtain an IP address automatically – Click this button to obtain the IP address automatically.
Router Name – Type in the router name provided by ISP.
Domain Name – Type in the domain name that you have assigned.
WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.



Specify an IP address – Click this radio button to specify some data.
IP Address – Type in the private IP address.
Subnet Mask – Type in the subnet mask.
Gateway IP Address – Type in gateway IP address.

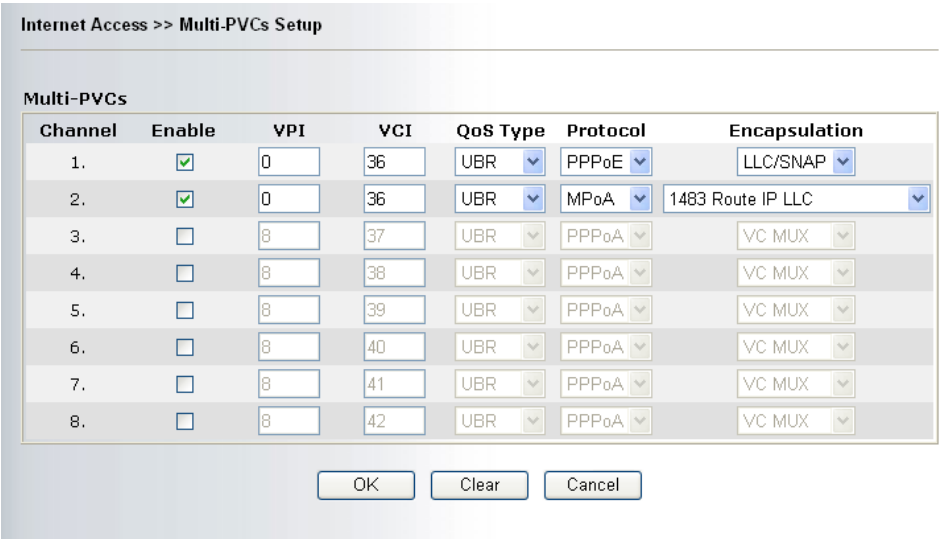
Default MAC Address — Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.
MAC Address – Type in the MAC address for the router manually.

DNS Server IP Address — Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

After finishing all the settings here, please click **OK** to activate them.

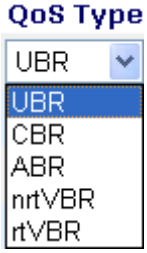
3.1.4 Multi-PVCs

This router allows you to create multi-PVCs for different data transferring for using. Simply go to **Internet Access** and select **Multi-PVC Setup** page.

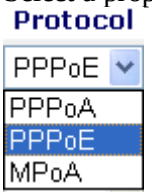


Enable — Type in the primary IP address for the router. If necessary, type

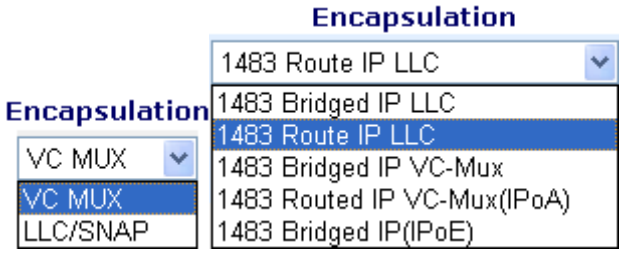
VPI	Type in the value provided by your ISP.
VCI	Type in the value provided by your ISP.
QoS Type	Select a proper QoS type for the channel.



Protocol	Select a proper protocol for this channel.



Encapsulation	Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.

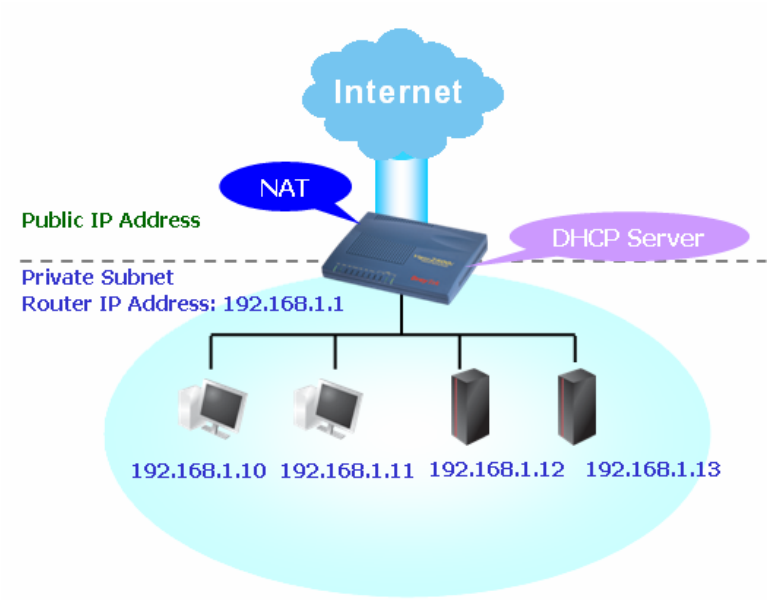


3.2 LAN

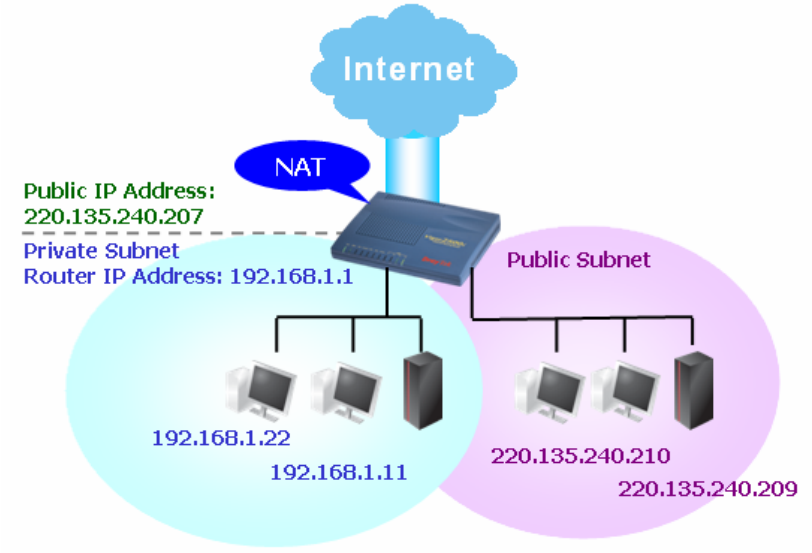
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

3.2.1 Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



What is Routing Information Protocol (RIP)

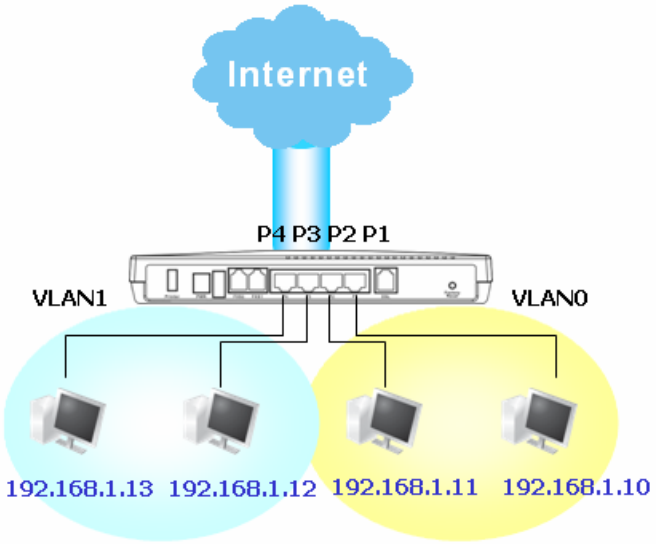
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

What are Virtual LANs

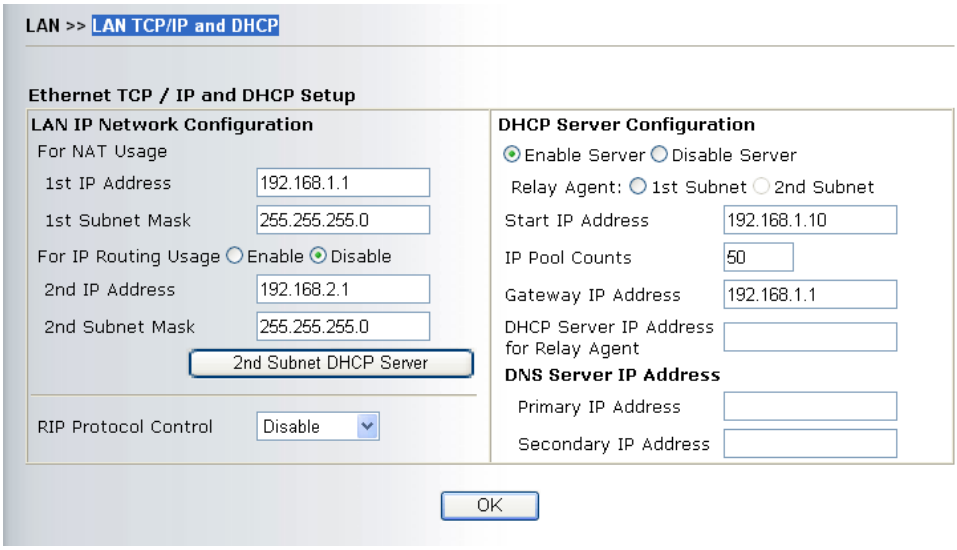
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



3.2.2 General Setup

This page provides you the general settings for LAN.

Click **LAN** to open the LAN settings page and choose **General Setup**.



1st IP Address Type in private IP address for connecting to a local private network (Default: 192.168.1.1).

1st Subnet Mask Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

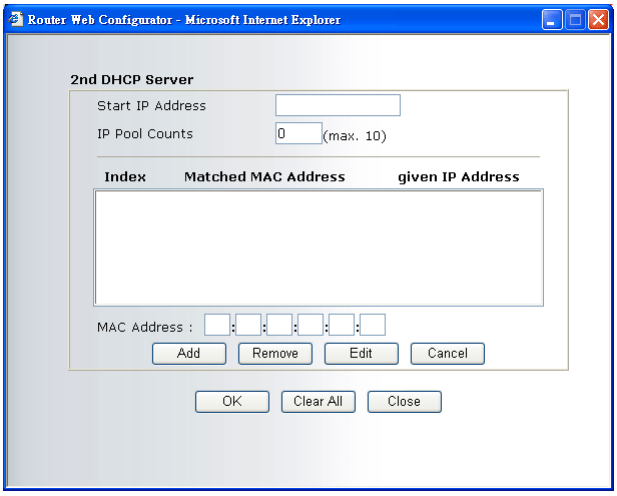
For IP Routing Usage Click **Enable** to invoke this function. The default setting is **Disable**.

2nd IP Address Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24)

2nd Subnet Mask An address code that determines the size of the network. (Default: 255.255.255.0/ 24)

2nd DHCP Server

You can configure the router to serve as a DHCP server for the 2nd subnet.



Start IP Address: Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control

Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.
2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

If you want to use another DHCP server in the network other than Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

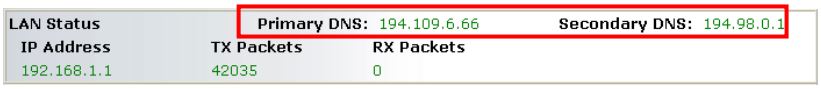
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address to every host in the LAN.
Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Force DNS manual setting -
Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

The default DNS Server IP address can be found via Online Status:



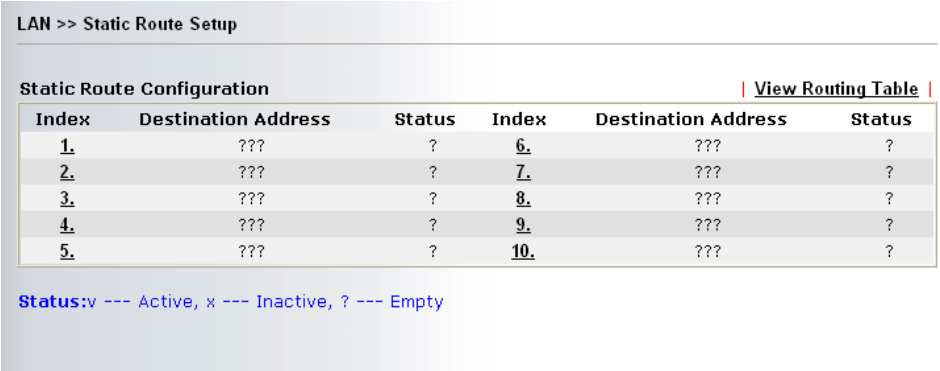
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

There are two common scenarios of LAN settings that stated in Chapter 4. For the configuration examples, please refer to that Chapter to get more information for your necessity.

3.2.3 Static Route

Go to **LAN** to open setting page and choose **Static Route**.

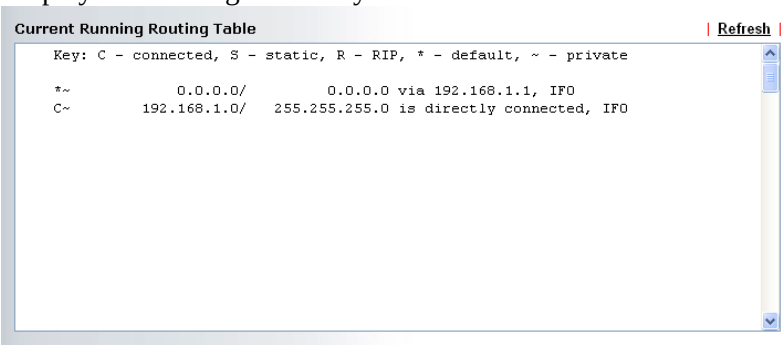


Index The number (1 to 10) under Index allows you to open next page to setup static route.

Destination Address Displays the destination address of the static route.

Status Displays the status of the static route.

Viewing Routing Table Displays the routing table for your reference.

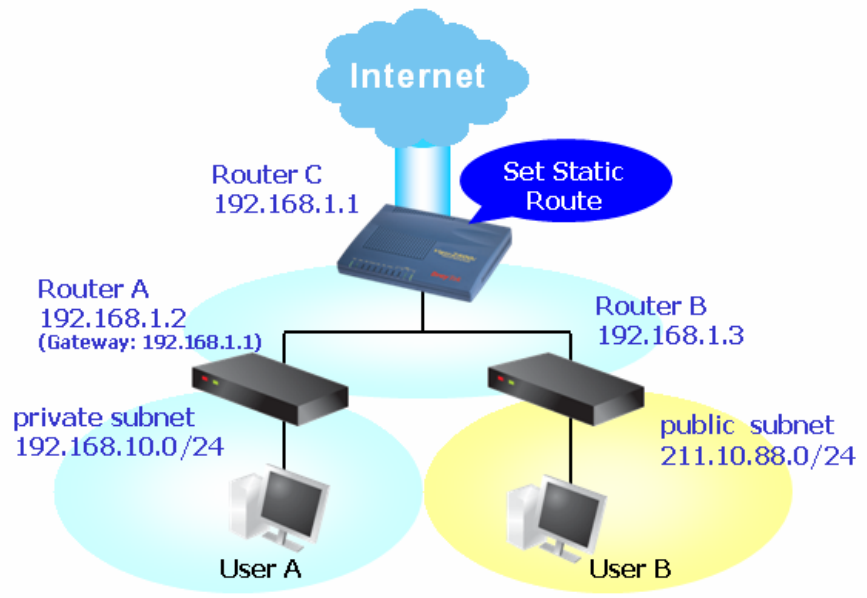


Add Static Routers to Private and Public Networks

Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.

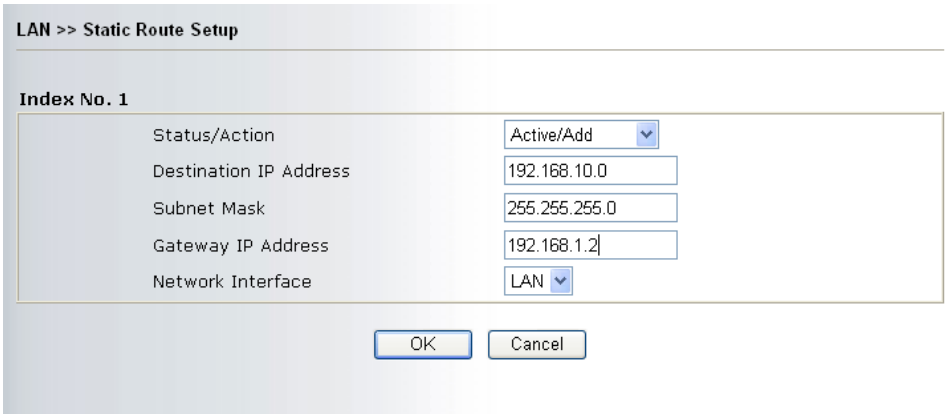


1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

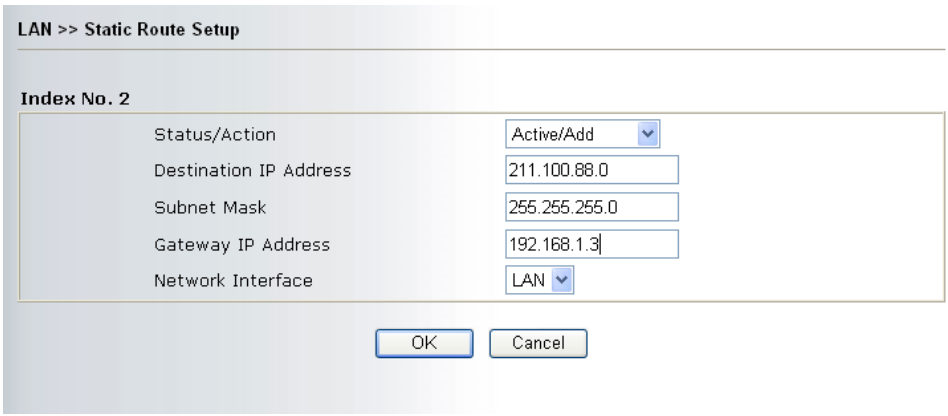
Note: There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via the router, and continuously exchange of IP routing information with different subnets.

---

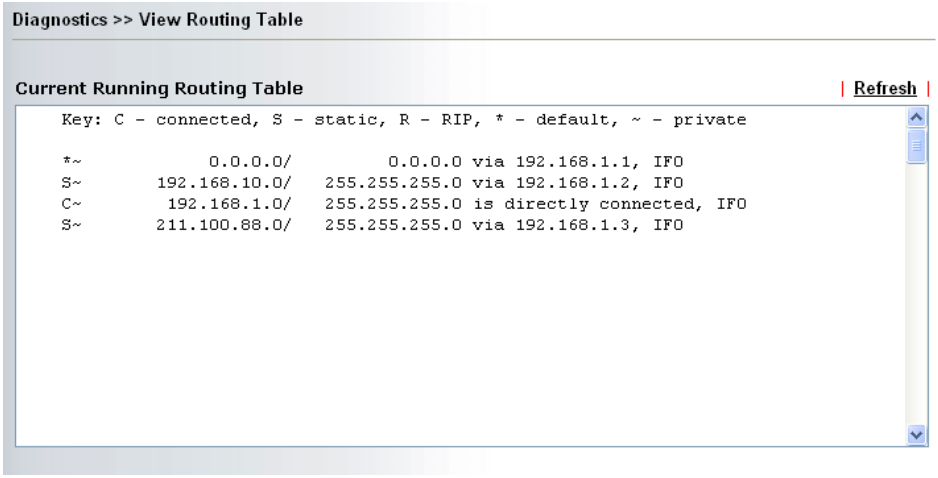
2. Click the **LAN - Static Route** and click on the **Index Number 1.** Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.2.

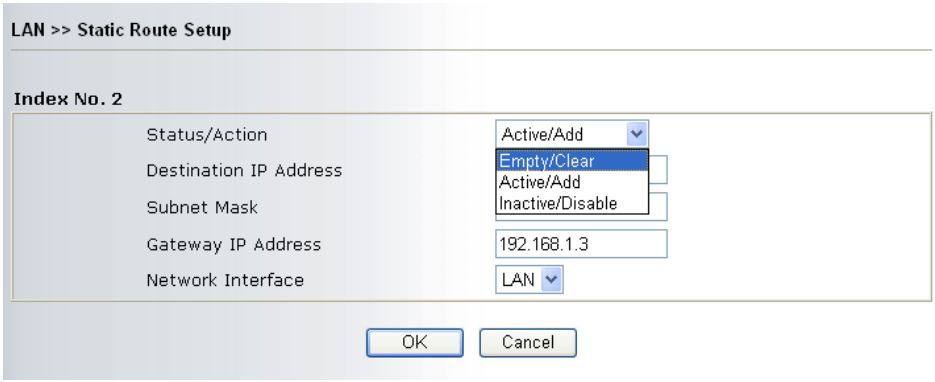


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



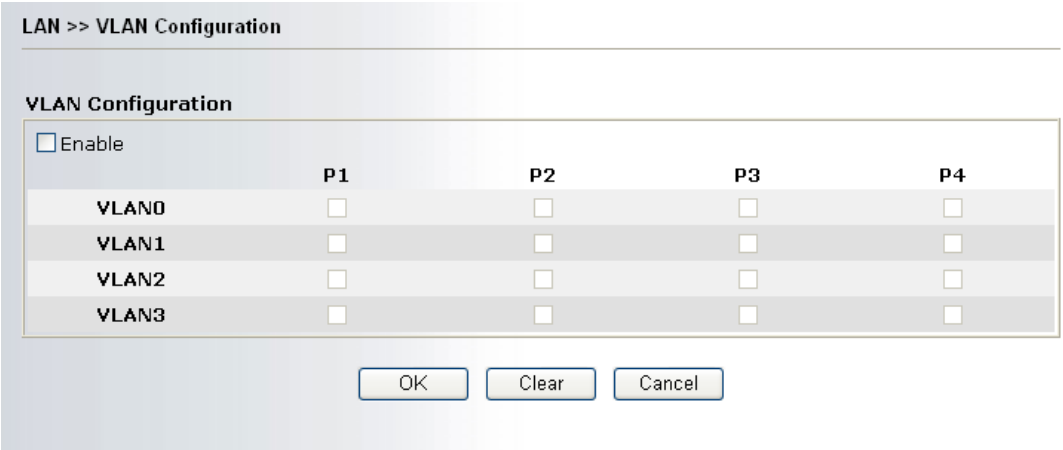
Delete or Deactivate Static Route

1. Go to **LAN** page and click **Static Route** to open the web page. Select the index number of the one that you want to delete.
2. Select **Empty/Clear** from the drop-down menu, and then click the **OK** button to delete the route.



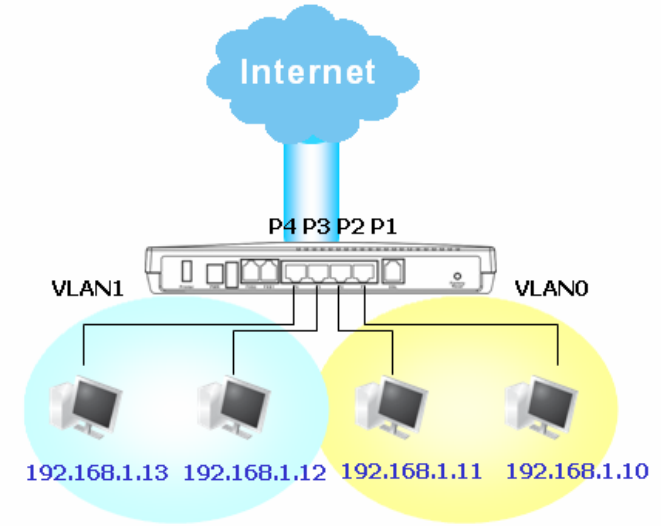
3.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to **LAN** menu and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

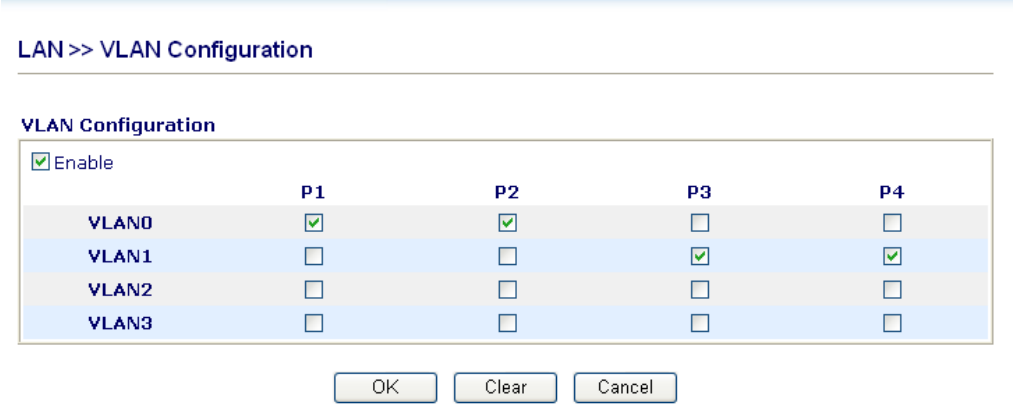


To add or remove a VLAN, please refer to the following example.

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4.



2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below.



3. To remove VLAN, uncheck the needed box and click **OK** to save the results.

3.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

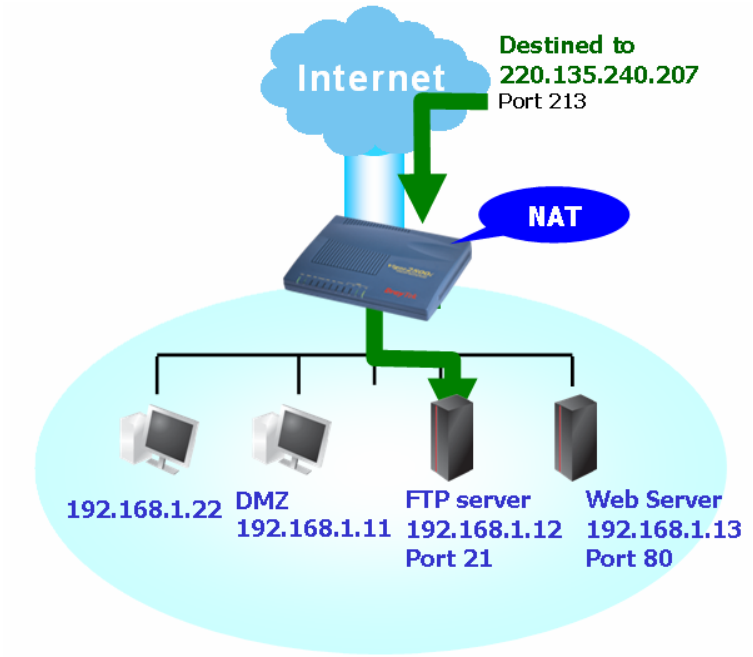
The benefit of the NAT includes:

- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

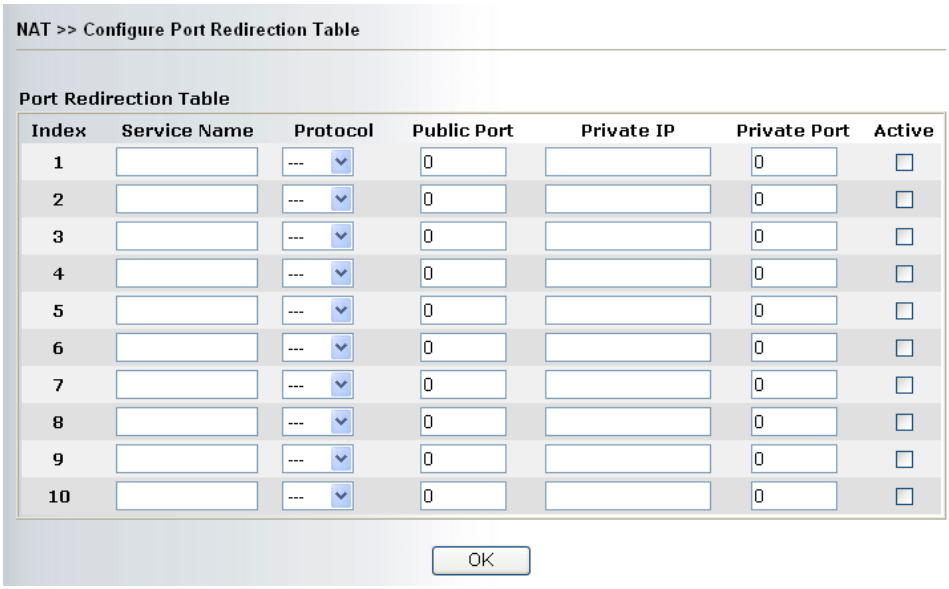
3.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic. The server users inside the LAN can not access public IP address of the server. The correct route is to access the server using the local private IP address of the server, or you should set up an alias in a Windows hosts file. Please only redirect the ports you know you have to forward rather than forward all ports. Otherwise, you will compromise the firewall-type security initially deployed by the NAT facility.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 10 port-mapping entries for the internal hosts.



Service Name Enter the description of the specific network service.

Protocol Select the transport layer protocol (TCP or UDP).

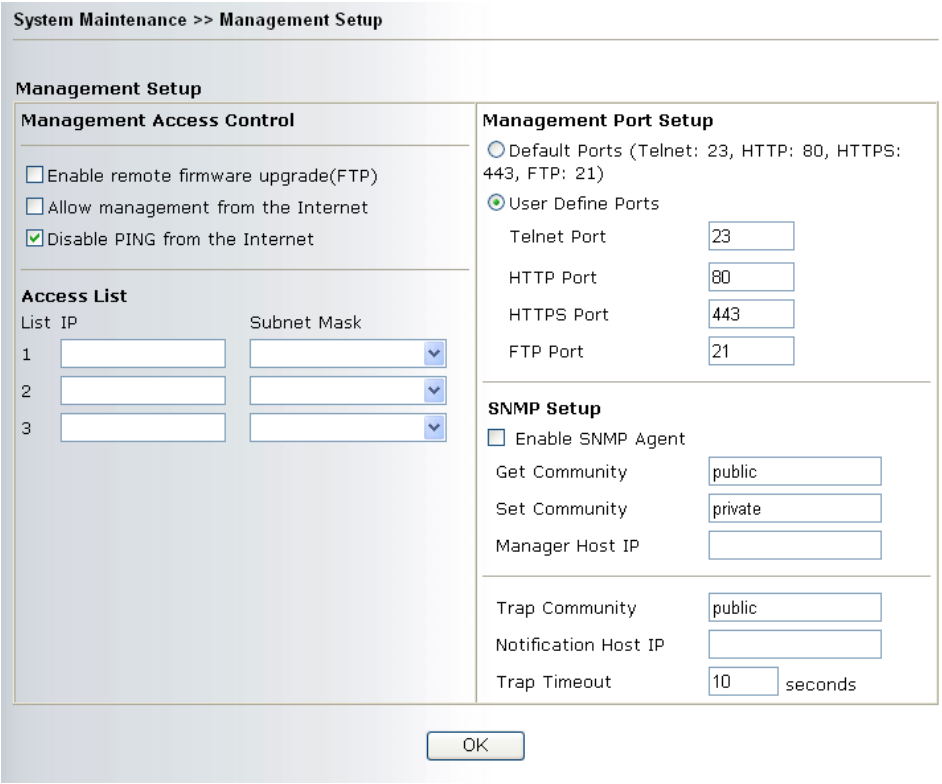
Public Port Specify which port can be redirected to the specified **Private IP and Port** of the internal host.

Private IP Specify the private IP address of the internal host providing the service.

Private Port	Specify the private port number of the service offered by the internal host.
Active	Check this box to activate the port-mapping entry you have defined.

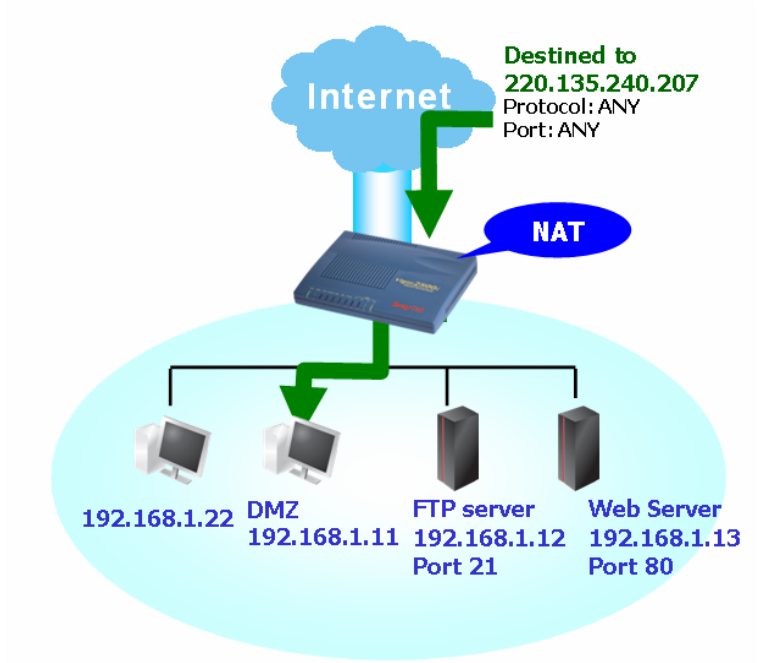
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router's in order to avoid confliction.

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.



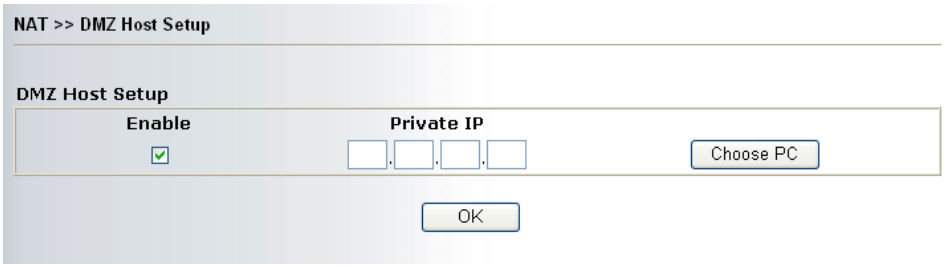
3.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page:

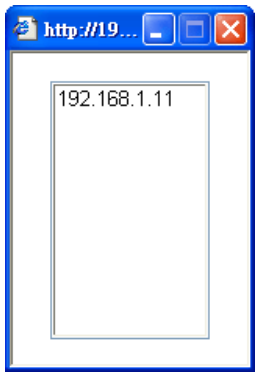


If you previously have set up **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA,** you will find them in **Aux. WAN IP list** for your selection.

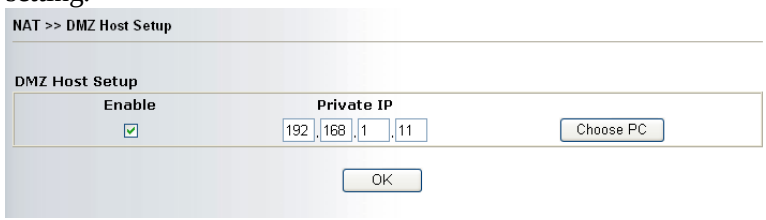
Enable Check to enable the DMZ Host function.

Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

Choose PC Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



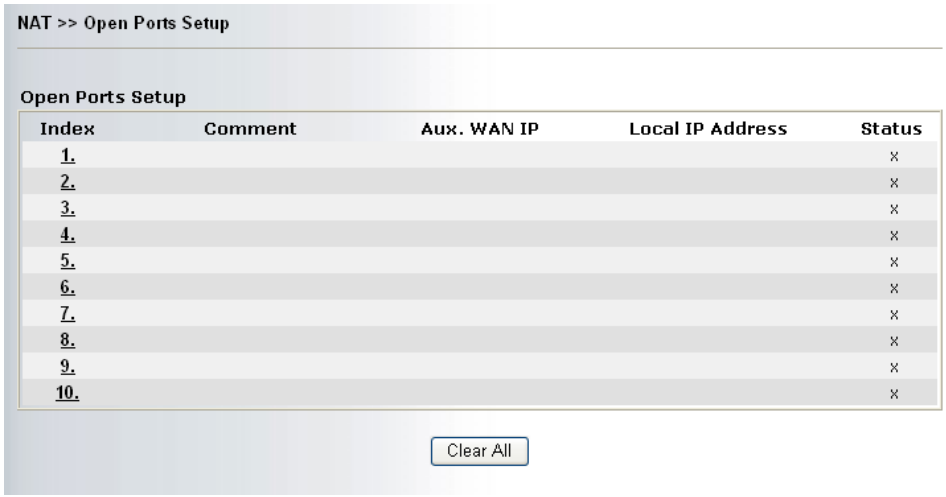
When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click OK to save the setting.



3.3.3 Open Ports

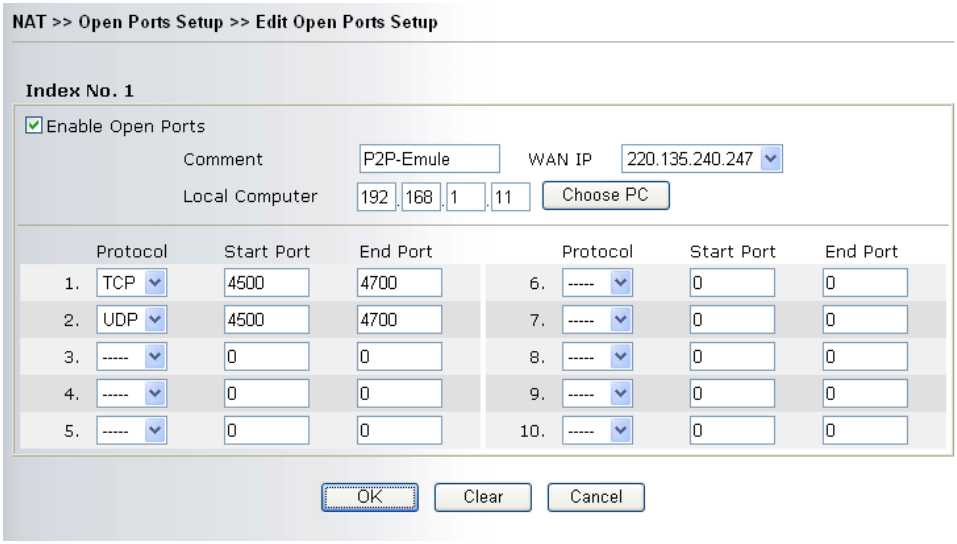
Open Ports allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

Click **Open Ports** to open the following page:



Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
Aux. WAN IP	Display the private IP address of the local host that you specify in WAN Alias.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.



However, if you previously have set up **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA,** you will find that **WAN IP** appeared for your selection.

Enable Open Ports Check to enable this entry.

Comment Make a name for the defined network application/service.

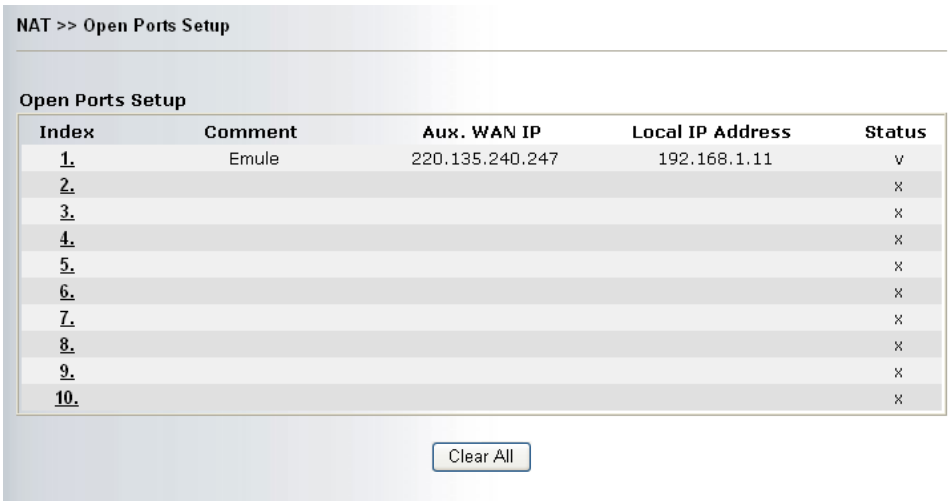
Local Computer Enter the private IP address of the local host or click Choose PC to select one.

Choose PC Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.

Protocol Specify the transport layer protocol. It could be **TCP**, **UDP**, or **-----** (none) for selection.

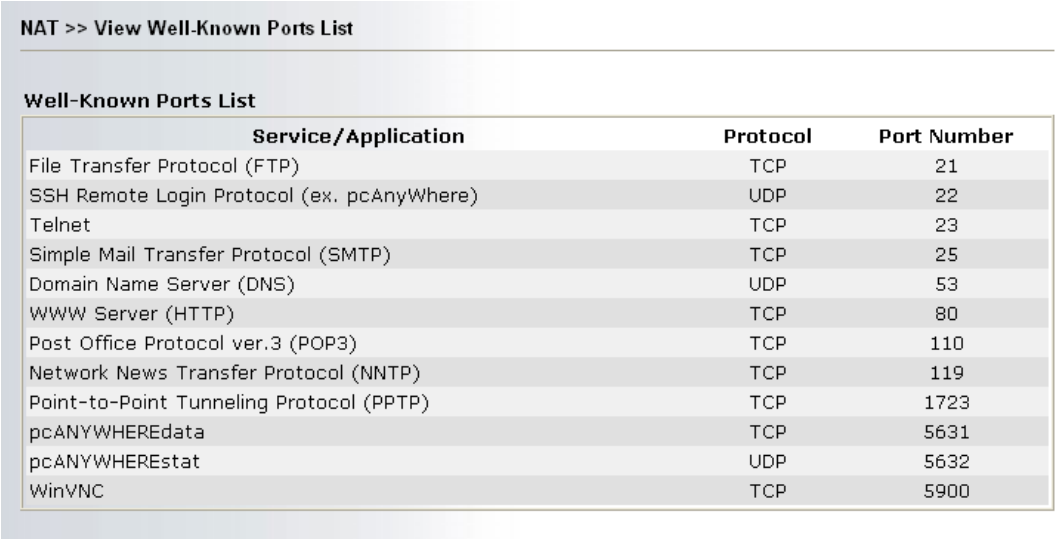
Start Port Specify the starting port number of the service offered by the local host.

End Port Specify the ending port number of the service offered by the local host.



3.3.4 Well-Known Ports List

This page provides you a view of well-known ports.



NAT >> View Well-Known Ports List

Well-Known Ports List

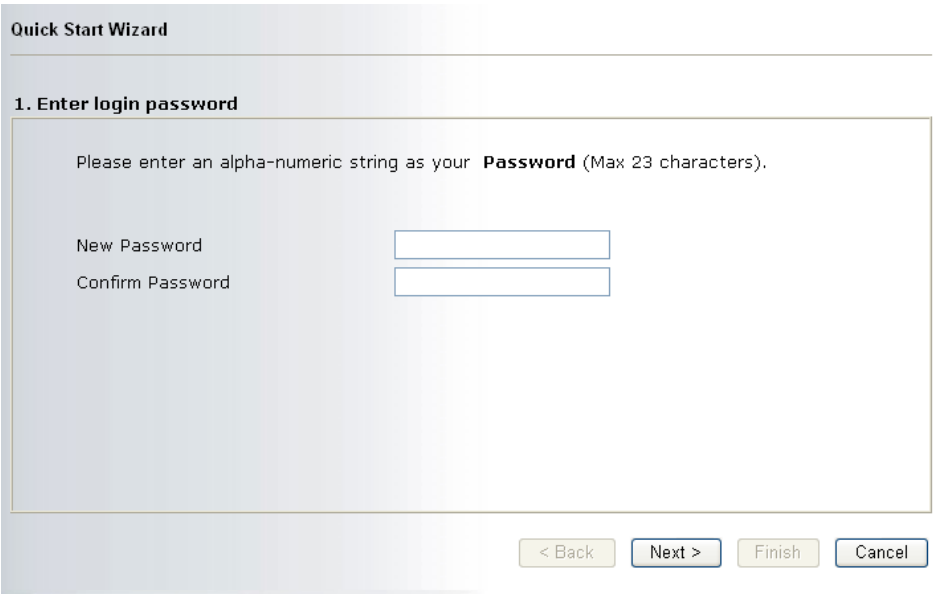
Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

3.4 Firewall

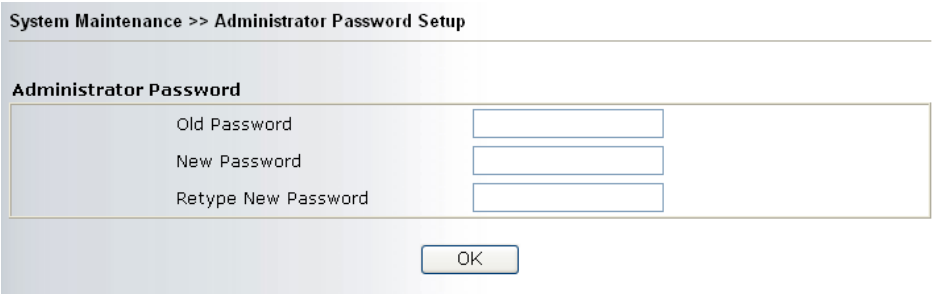
3.4.1 Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

The most basic security concept is to set user name and password while you install your router. The administrator login will prevent unauthorized access to the router configuration from your router.



If you did not set password during installation; you can go to **System Maintenance** to set up your password.



Firewall Facilities

The users on the LAN are provided with secured protection by the following firewall facilities:

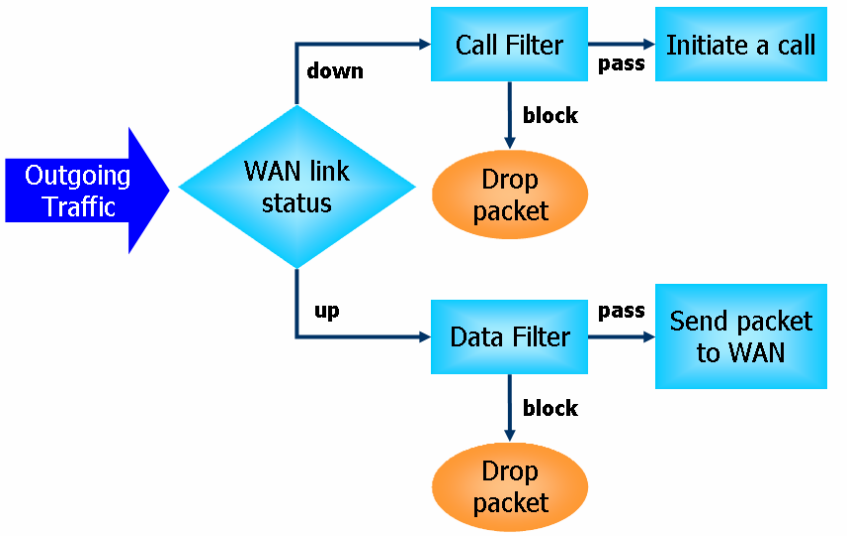
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

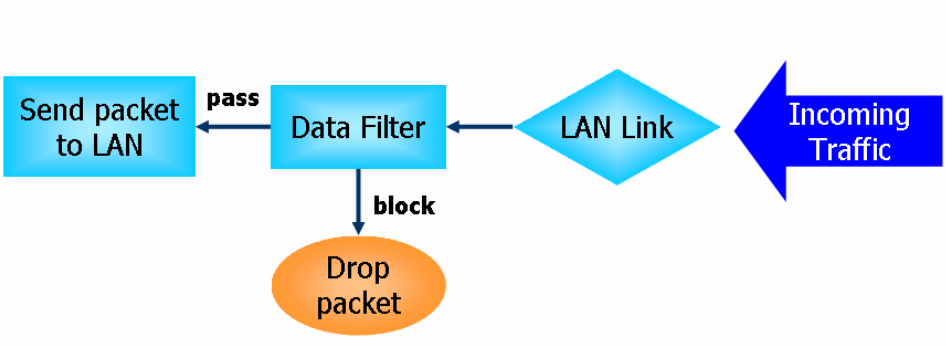
IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter** - When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.





Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not just examine the header information also monitor the state of the connection.

Instant Messenger (IM) and Peer-to-Peer (P2P) Application Blocking

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide IM and P2P blocking functionality.

Denial of Service (DoS) Defense

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

The below shows the attack types that DoS/DDoS defense function can detect:

1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. TCP Flag scan
5. Trace route
6. IP options
7. Unknown protocol
8. Land attack
9. Smurf attack
10. SYN fragment
11. ICMP fragment
12. Tear drop attack
13. Fraggle attack
14. Ping of Death attack
15. TCP/UDP port scan

Content Filtering

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Filtering

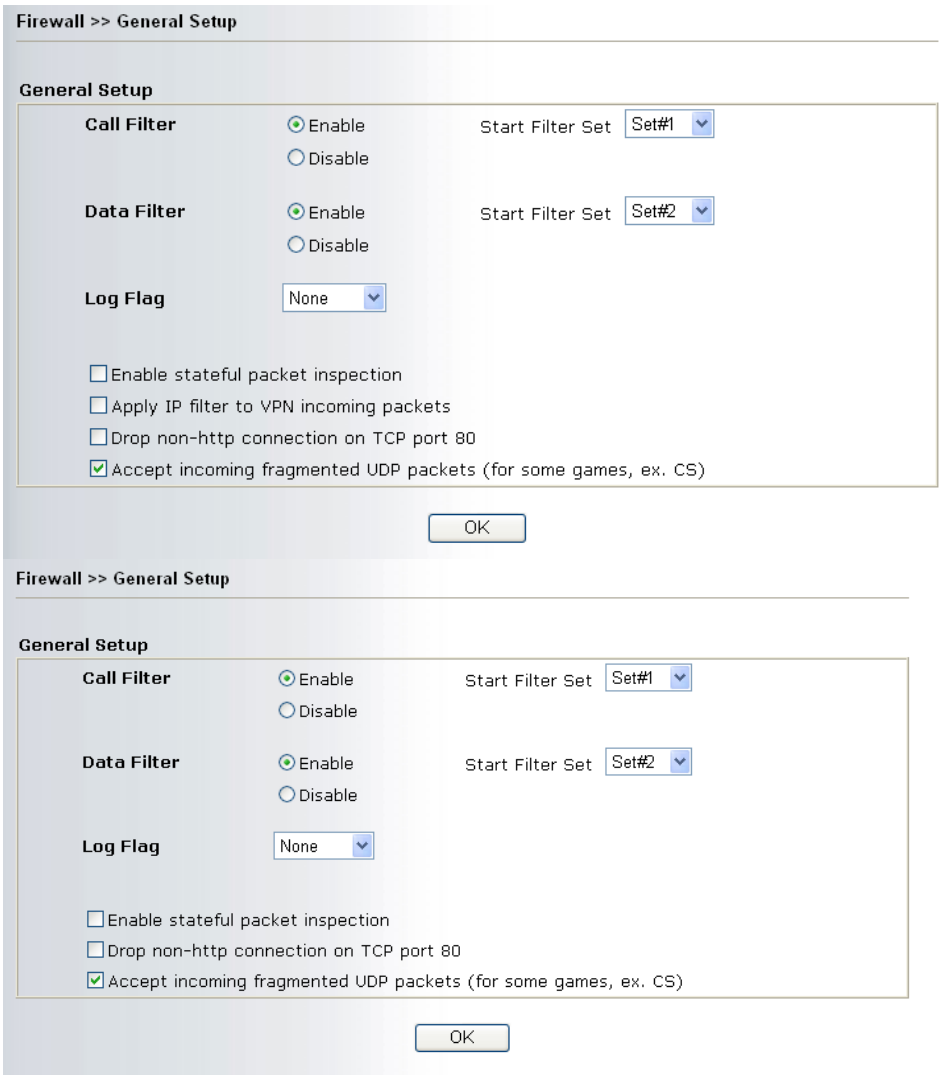
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database, powered by SurfControl. The database covering over 70 languages and 200 countries, over 1 billion Web pages divided into 40 easy-to-understand categories. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

3.4.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Enable Stateful packet inspection**, **Drop non-http connection on TCP port 80**, and **Accept incoming fragmented UDP packets**.

Click **Firewall** and click **General Setup** to open the general setup page.

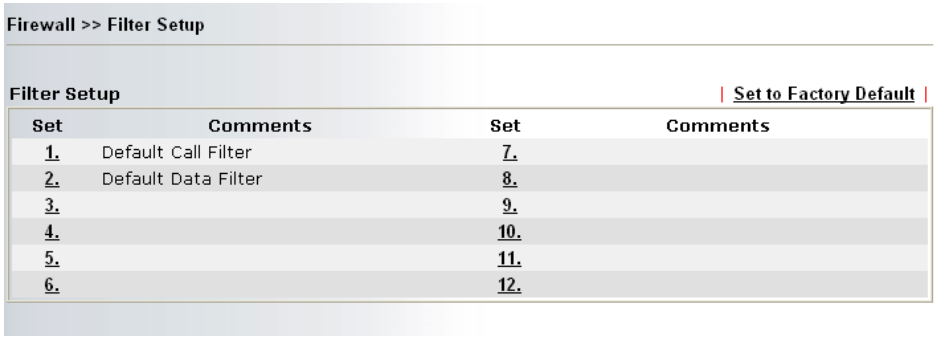


Call Filter	Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.
Log Flag	For troubleshooting needs you can specify the filter log here. **None -** The log function is not activated. **Block -** All blocked packets will be logged. **Pass -** All passed packets will be logged. **No Match -** The log function will record all packets that are not matched. Note that the filter log will be displayed on the Telnet terminal when you type the ***log -f*** command.

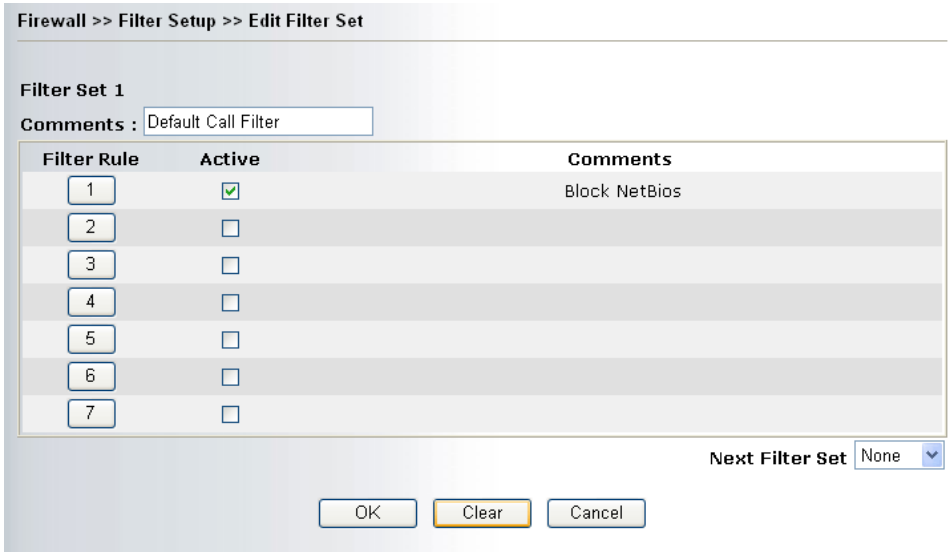
Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable “Accept Incoming Fragmented UDP Packets”. By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable “Accept Incoming Fragmented UDP Packets”.

3.4.3 Filter Setup

Click **Firewall** and click **Filter Setup** to open the setup page.



To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.



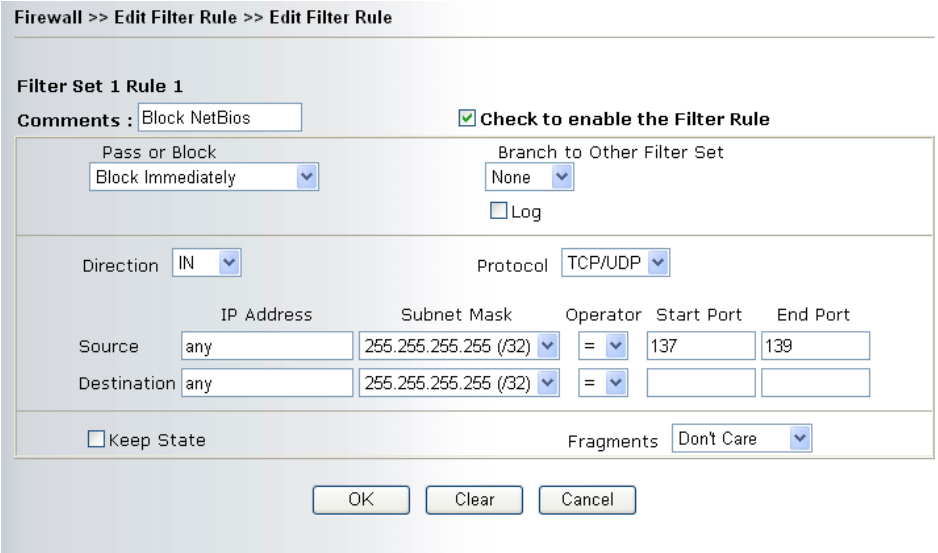
Filter Rule — Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.

Active — Enable or disable the filter rule.

Comment — Enter filter set comments/description. Maximum length is 23–character long

Next Filter Set — Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

To edit **Filter Rule**, click the **Filter Rule** index button to enter the Filter Rule setup page.



Comments — Enter filter set comments/description. Maximum length is 14-character long.

Check to enable the Filter Rule — Check this box to enable the filter rule.

Pass or Block — Specifies the action to be taken when packets match the rule.
Block Immediately - Packets matching the rule will be dropped immediately.
Pass Immediately - Packets matching the rule will be passed immediately.
Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.
Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.

Branch to other Filter Set — If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu.

Log — Check this box to enable the log function. Use the Telnet command ***log-f*** to view the logs.

Direction — Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic.

Protocol — Specify the protocol(s) which this filter rule will apply to.

IP Address — Specify a source and destination IP address for this filter rule to apply to. Place the symbol "!" before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter **any** or leave the field blank.

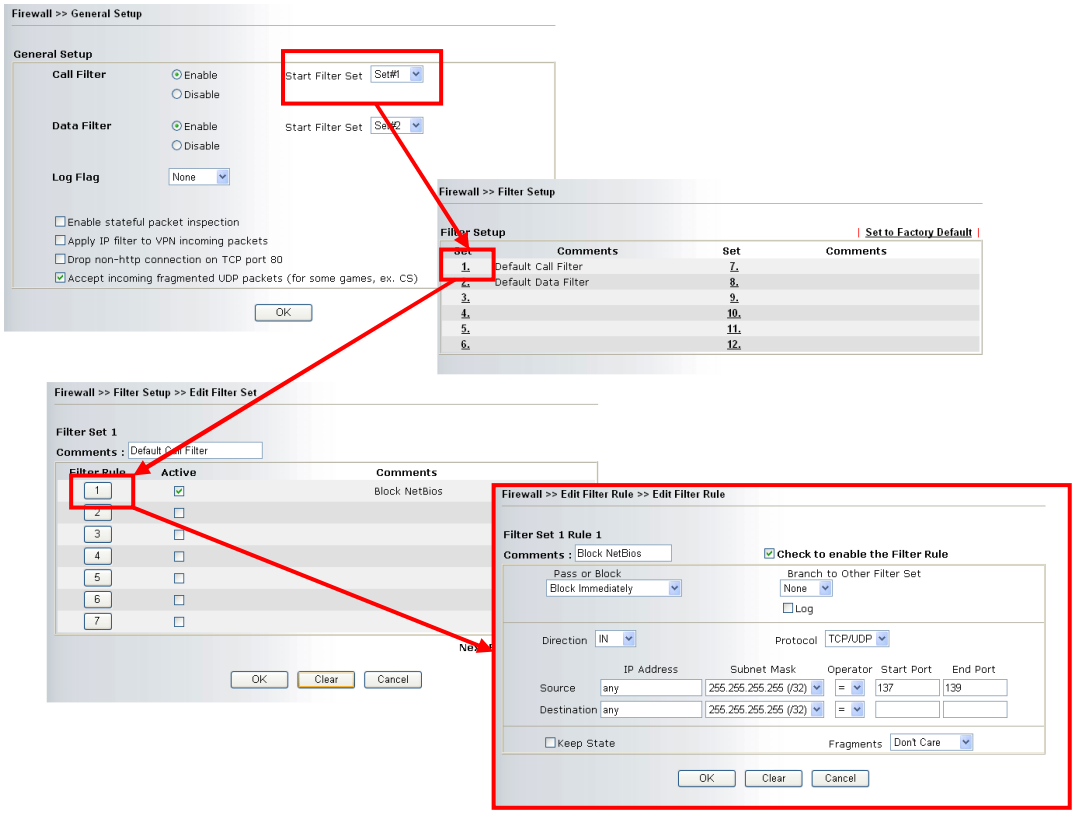
Subnet Mask — Select the **Subnet Mask** for the IP Address column for this filter rule to apply from the drop-down menu.

Operator, Start Port and End Port — The operator column specifies the port number settings. If the **Start Port** is empty, the **Start Port** and the **End Port** column will be ignored. The filter rule will filter out any port number.
(=) If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including

	the Start Port and the End Port). ***(!=)***If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port). ***(>)*** Specify the port number is larger than the Start Port (includes the Start Port). ***(<)*** Specify the port number is less than the Start Port (includes the Start Port).
Keep State	This function should work along with Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port settings. It is used for Data Filter only. Keep State is in the same nature of modern term Stateful Packet Inspection. It tracks packets, and accept the packets with appropriate characteristics showing its state is legal as the protocol defines. It will deny unsolicited incoming data. You may select protocols from any, TCP, UDP, TCP/UDP, ICMP and IGMP.
Fragments	Specify the action for fragmented packets. And it is used for **Data Filter** only. ***Don't care*** **-**No action will be taken towards fragmented packets. ***Unfragmented*** **-**Apply the rule to unfragmented packets. ***Fragmented*** **-** Apply the rule to fragmented packets. ***Too Short*** **-** Apply the rule only to packets that are too short to contain a complete header.

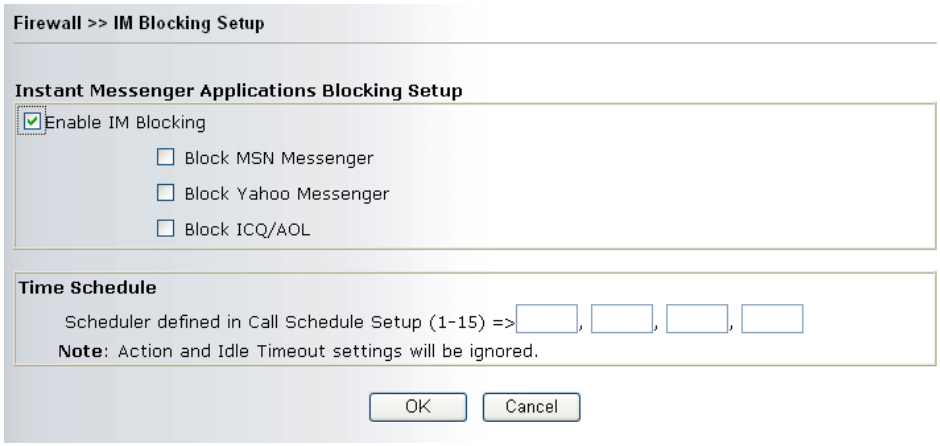
Example

As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



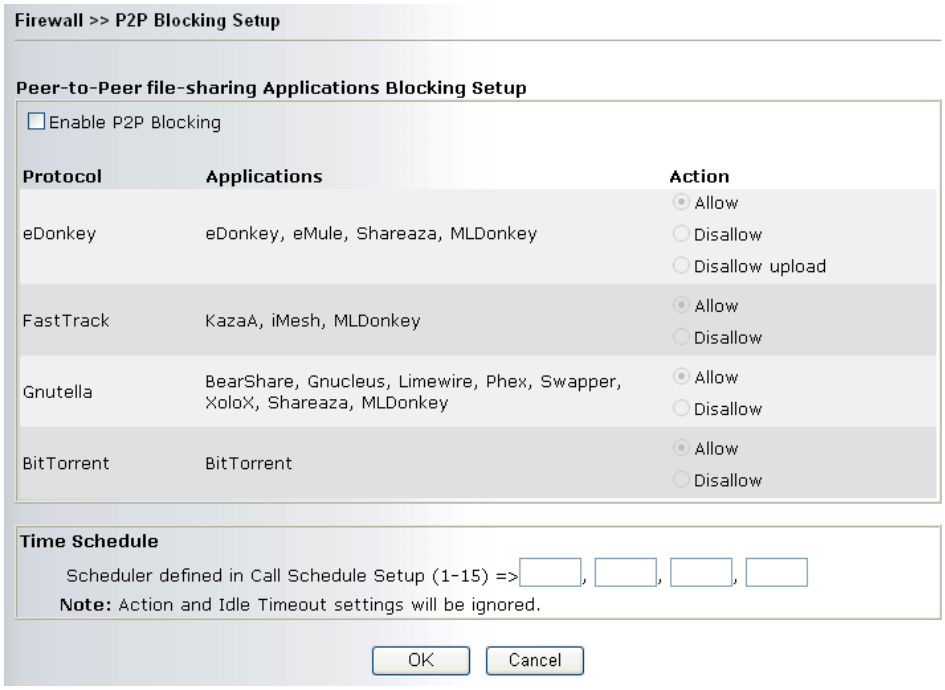
3.4.4 IM Blocking

IM Blocking means instant messenger blocking. Click **Firewall** and click **IM Blocking** to open the setup page. You will see a list of common IM (such as MSN, Yahoo, ICQ/AQL) applications. Check **Enable IM Blocking** and select the one(s) that you want to block. To block selected IM applications during specific periods, enter the number of the scheduler predefined in **Applications>>Call Schedule**.



3.4.5 P2P Blocking

P2P is the short name of peer to peer. Click **Firewall** and click **P2P Blocking** to open the setup page. You will see a list of common P2P applications. Check **Enable P2P Blocking** and select the one(s) to block. To block selected P2P applications during specific periods, enter the number of the scheduler predefined in **Applications>>Call Schedule**.

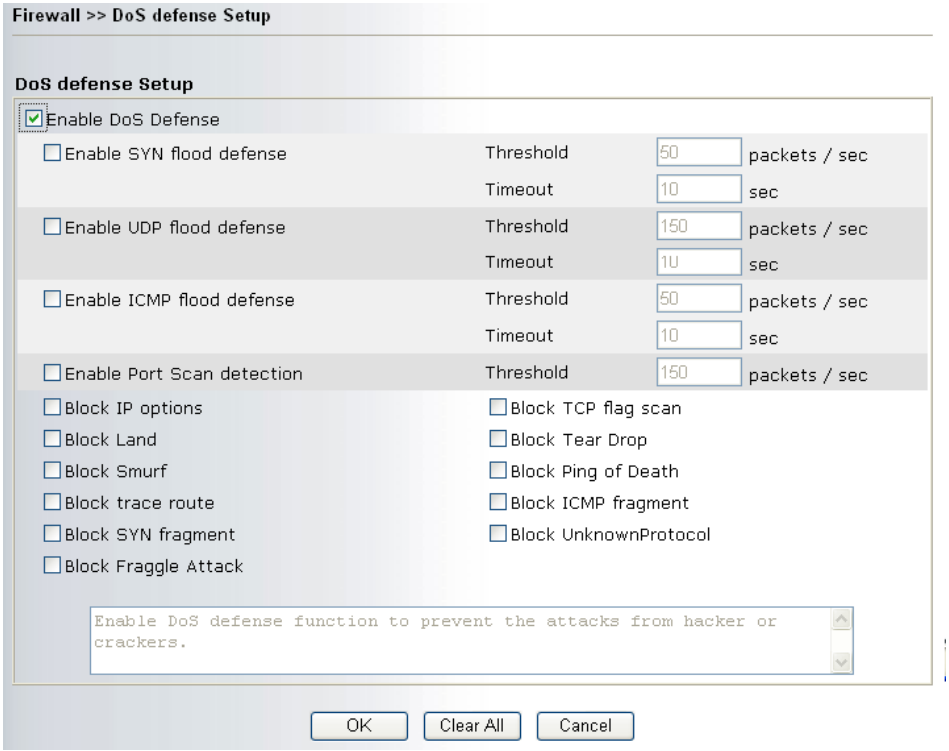


Action Specify the action for each protocol.
Allow – Allow the client to access into the application through the specified protocol.
Disallow – Forbid the client to access into the application through the specified protocol.
Disallow upload – Forbid the client to access into the application through the specified protocol for downloading. Yet uploading is allowed.

3.4.6 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

Click **Firewall** and click **DoS Defense** to open the setup page.



Enable Dos Defense Check the box to activate the DoS Defense Functionality.

Enable SYN flood defense Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.

Enable UDP flood defense Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.

Enable ICMP flood defense Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.

Enable PortScan detection Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the

	port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include ***no flag scan***, ***FIN without ACK scan***, ***SYN FINscan***, ***Xmas scan*** and ***full Xmas scan***.
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed

SYN packets with the identical source and destination addresses, as well as the port number to victims.

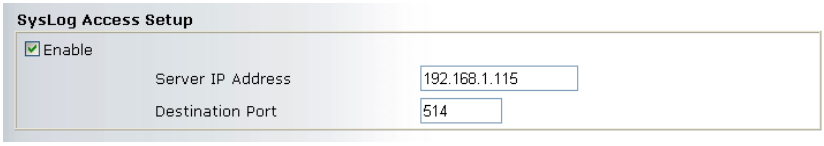
Block Unknown Protocol

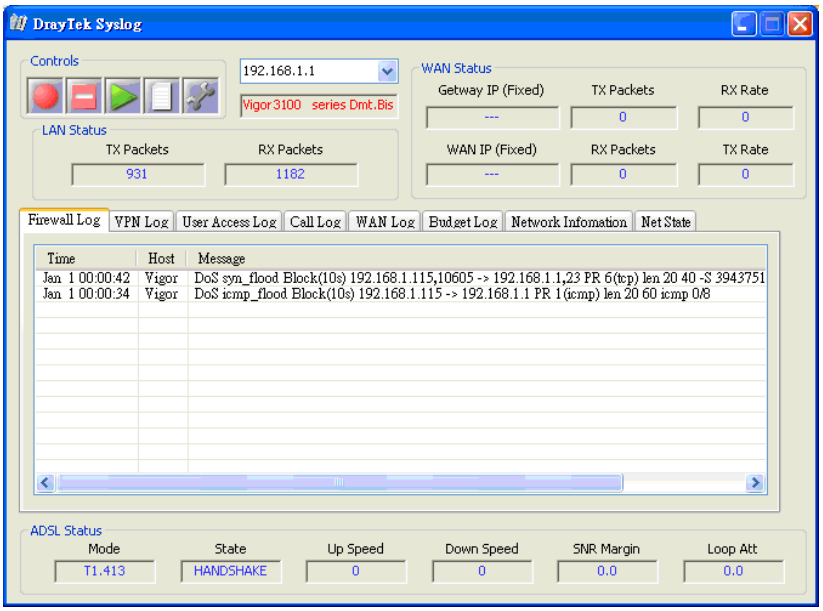
Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.

Warning Messages

We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. (Refer to Chapter 13 System Maintenance Syslog Access Setup for detail information.)

All the warning messages related to **DoS defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.





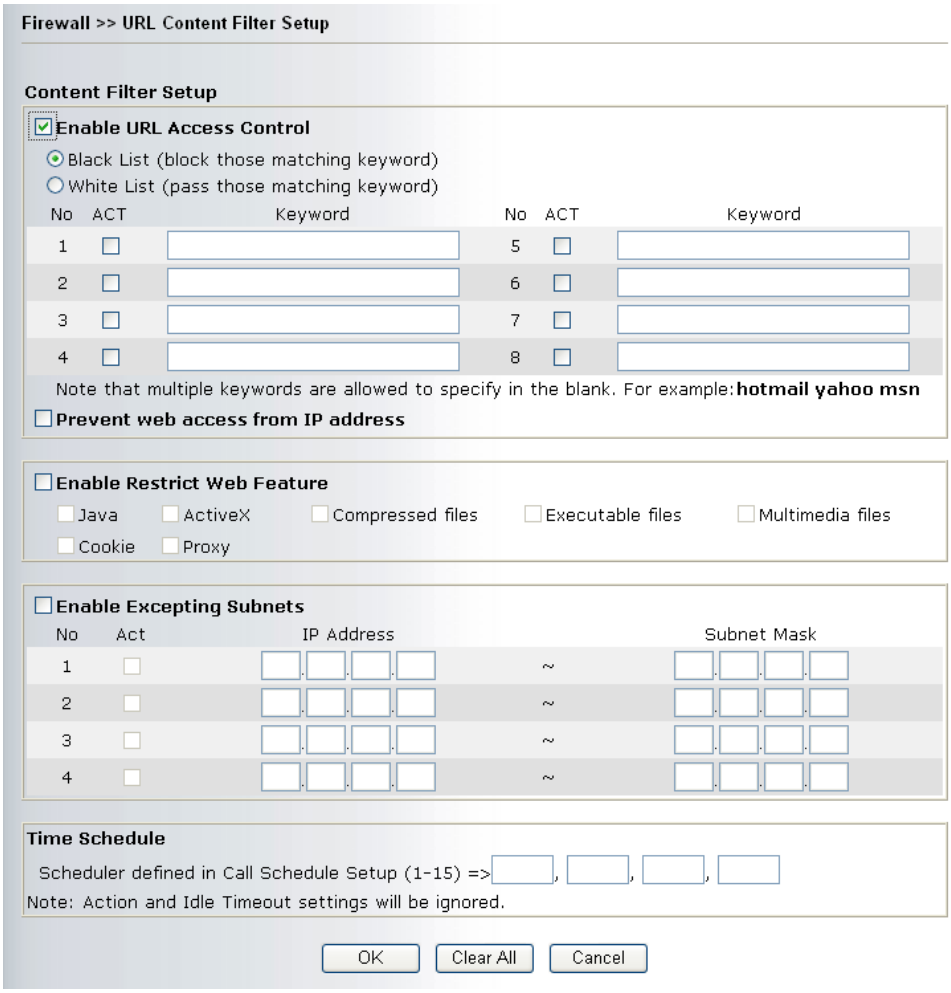
3.4.7 URL Content Filter

Based on the list of user defined keywords, the **URL Content Filter** facility in Vigor router inspects the URL string in every outgoing HTTP request. No matter the URL string is found full or partial matched with a keyword, the Vigor router will block the associated HTTP connection.

For example, if you add key words such as “sex”, Vigor router will limit web access to web sites or web pages such as “www.sex.com”, ”www.backdoor.net/images/sex/p_386.html”. Or you may simply specify the full or partial URL such as “www.sex.com” or “sex.com”.

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click **Firewall** and click **URL Content Filter** to open the setup page.



Enable URL Access Control	Check the box to activate URL Access Control.
Black List (block those matching keyword)	Click this button to restrict accessing into the corresponding webpage with the keywords listed on the box below.
White List (pass those matching keyword)	Click this button to allow accessing into the corresponding webpage with the keywords listed on the box below.
Keyword	The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.
Prevent web access from IP address	Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

Enable Restrict Web Feature	Check the box to activate the function. ***Java -*** Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet. ***ActiveX -*** Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused. ***Compressed file -*** Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router. . **zip, rar, .arj, .ace, .cab, .sit** ***Executable file -*** Check the box to reject any downloading behavior of the executable file from the Internet. **.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg** ***Cookie -*** Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. ***Proxy -*** Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router. **.mov .mp3 .rm .ra .au .wmv** **.wav .asf .mpg .mpeg .avi .ram**
Enable Excepting Subnets	Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the ***URL Access Control***. To enable an entry, click on the empty checkbox, named as **ACT**, in front of the appropriate entry.
Time Schedule	Specify what time should perform the URL content filtering facility.

3.4.8 Web Content Filter

Click **Firewall** and click **Web Content Filter** to open the setup page.

For this section, please refer to **Web Content Filter** user's guide for detailed information.

3.5 Applications

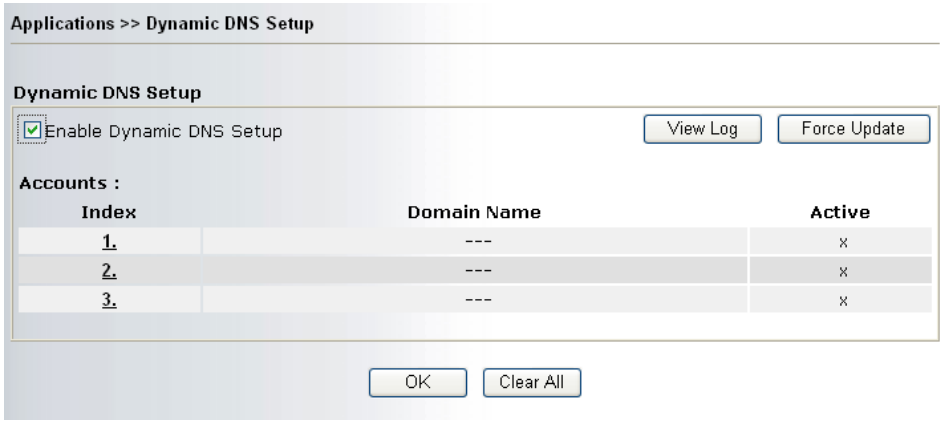
3.5.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

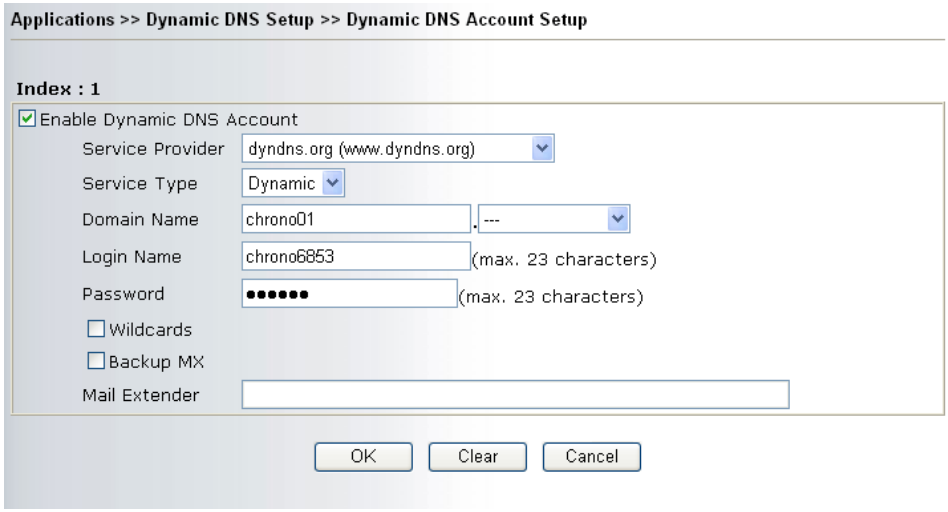
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** You should visit their websites to register your own domain name for the router.

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say ***hostname.dyndns.org***, and an account with username: ***test*** and password: ***test***.
2. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.



3. Select Index number 1 to add an account for the router. Check Enable Dynamic DNS Account, and choose correct Service Provider: dyndns.org, type the registered hostname: ***hostname*** and domain name suffix: dyndns.org in the Domain Name block. The following two blocks should be typed your account Login Name: ***test*** and Password: ***test***.



Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom, Static).
Domain Name	Type in a domain name that you applied previously.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

4. Click **OK** button to activate the settings. You will see your setting has been saved.

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

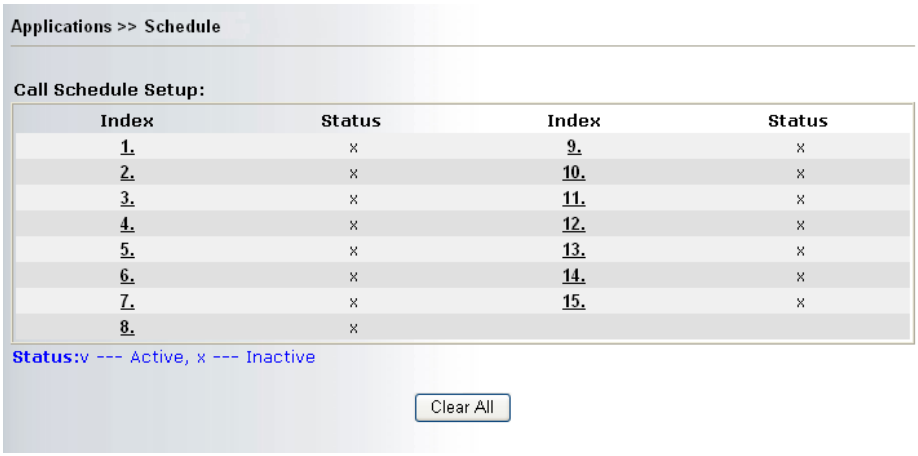
Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.5.2 Schedule

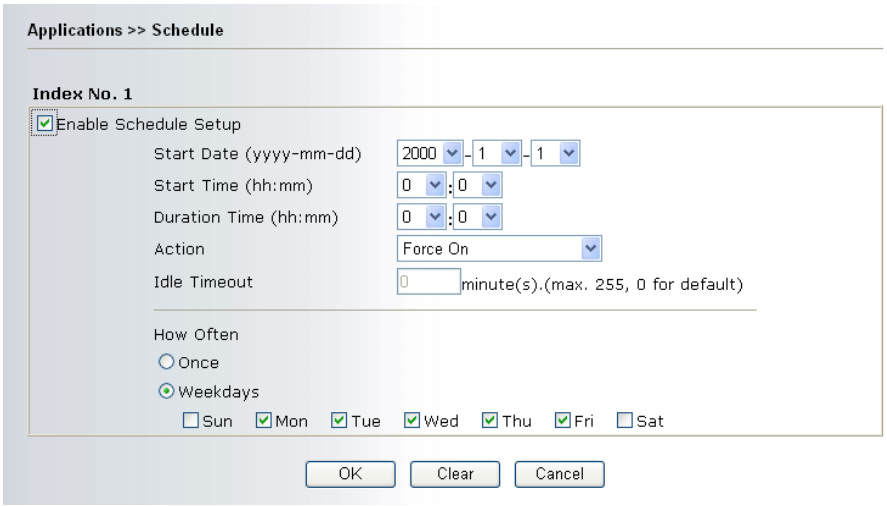
The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time Setup** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.



You can set up to 15 schedules. Then you can apply them to your **Internet Access**.

To add a schedule, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.



Enable Schedule Setup Check to enable the schedule.

Start Date (yyyy-mm-dd) Specify the starting date of the schedule.

Start Time (hh:mm) Specify the starting time of the schedule.

Duration Time (hh:mm) Specify the duration (or period) for the schedule.

Action	Specify which action Call Schedule should apply during the period of the schedule. **Force On -**Force the connection to be always on. **Force Down -**Force the connection to be always down. **Enable Dial-On-Demand -**Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field. **Disable Dial-On-Demand -**Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule. **How often -**Specify how often the schedule will be applied **Once -**The schedule will be applied just once **Weekdays -**Specify which days in one week should perform the schedule.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).

Office Hour:

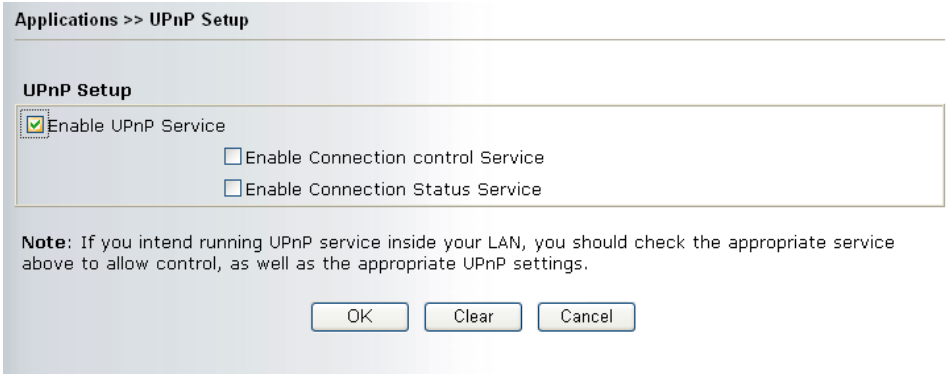
(Force On)

Mon - Sun **9:00 am** **to** **6:00 pm**

1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

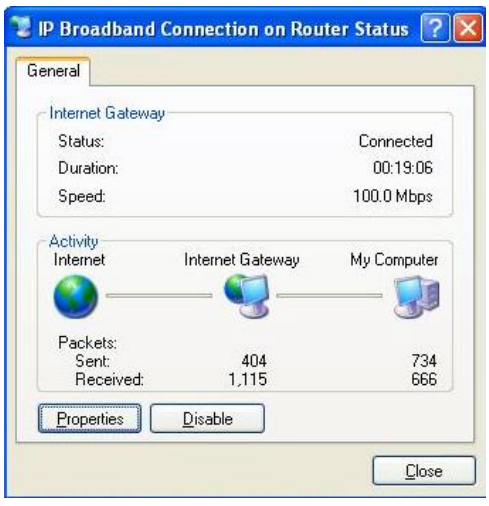
3.5.3 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

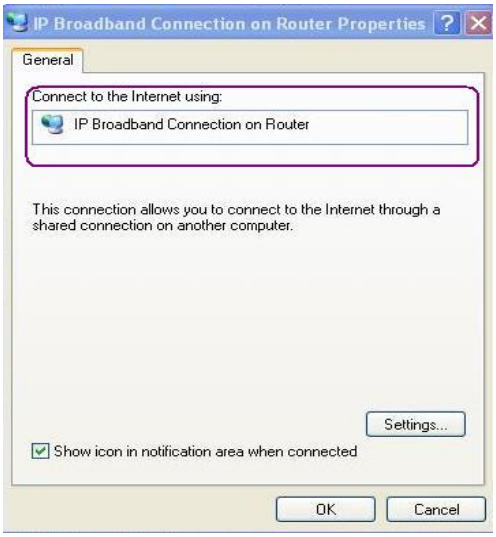


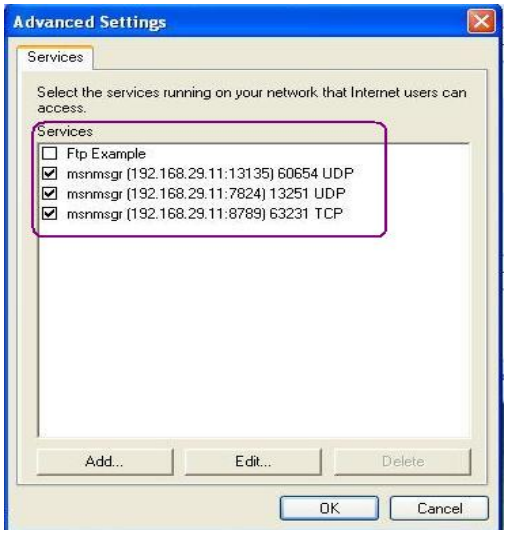
Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.



The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.





The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

3.6 Wireless LAN

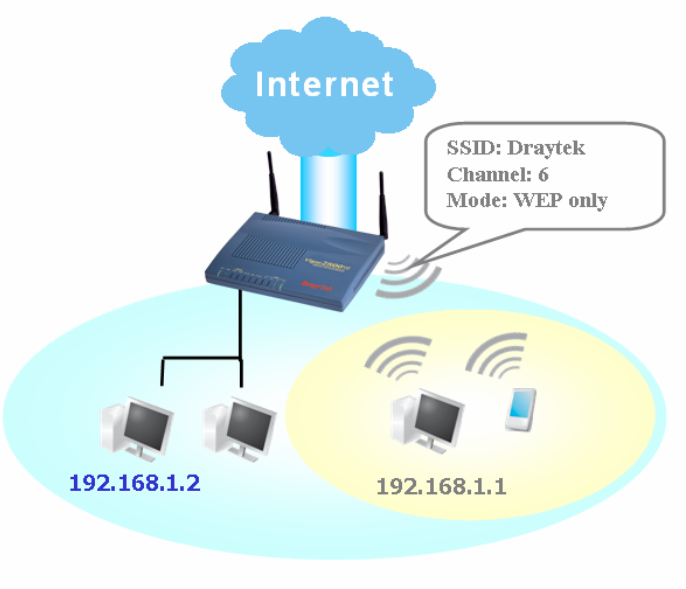
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor Ge model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11g protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology Super G ™ to lift up data rate up to 108 Mbps (The actual data throughput will vary according to the network conditions and environmental

factors, including volume of network traffic, network overhead and building materials). Hence, you can finally smoothly enjoy stream music and video.

3.8.1 Basic Concept

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection with other wired hosts via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Real-time Hardware Encryption

Vigor Router is equipped with a hardware AES encryption engine so it can apply highest protection to your data without influencing user experience.

Complete Security Standard Selection

To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

- WEP (Wireless Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.
- Wi-Fi Protected Access, the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.
- In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

  Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs.

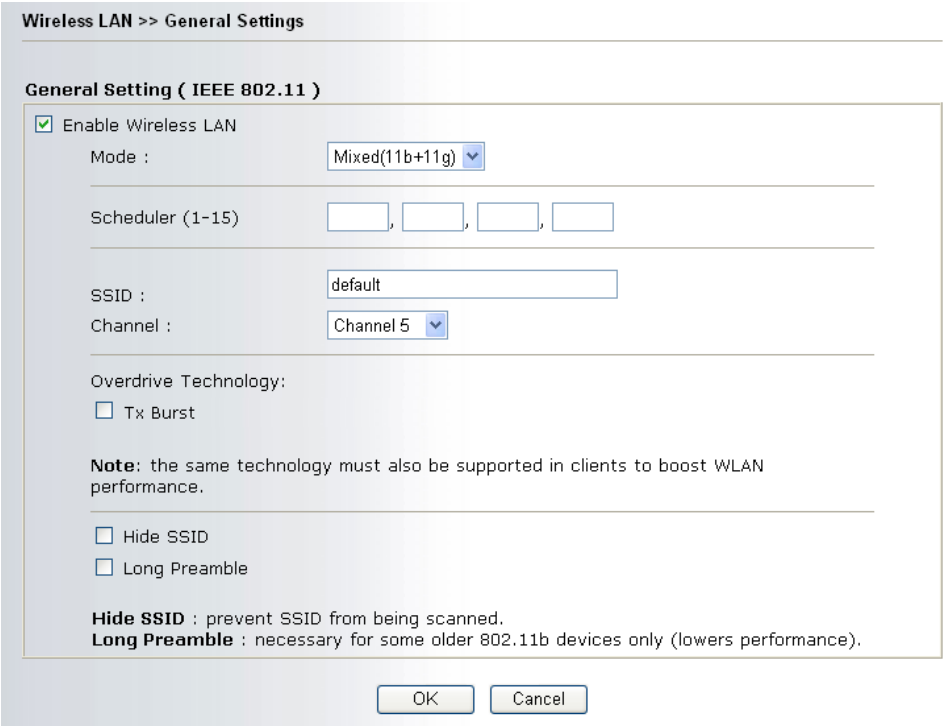
No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless networks. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time. Below shows three examples for your reference.

Station List will display all the station in your wireless network and the status of their connection. Besides, you can allow the connection of only trusted user with the function **MAC Access control**. **Station Rate Control** can assign specific download/upload rate to each STA.

WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add a filter of MAC address to isolate single user's access from wired LAN.

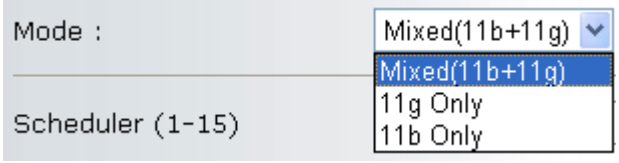
3.6.2 General Settings

This web page allows you to enable wireless LAN function.



Enable Wireless LAN Check the box to enable wireless function.

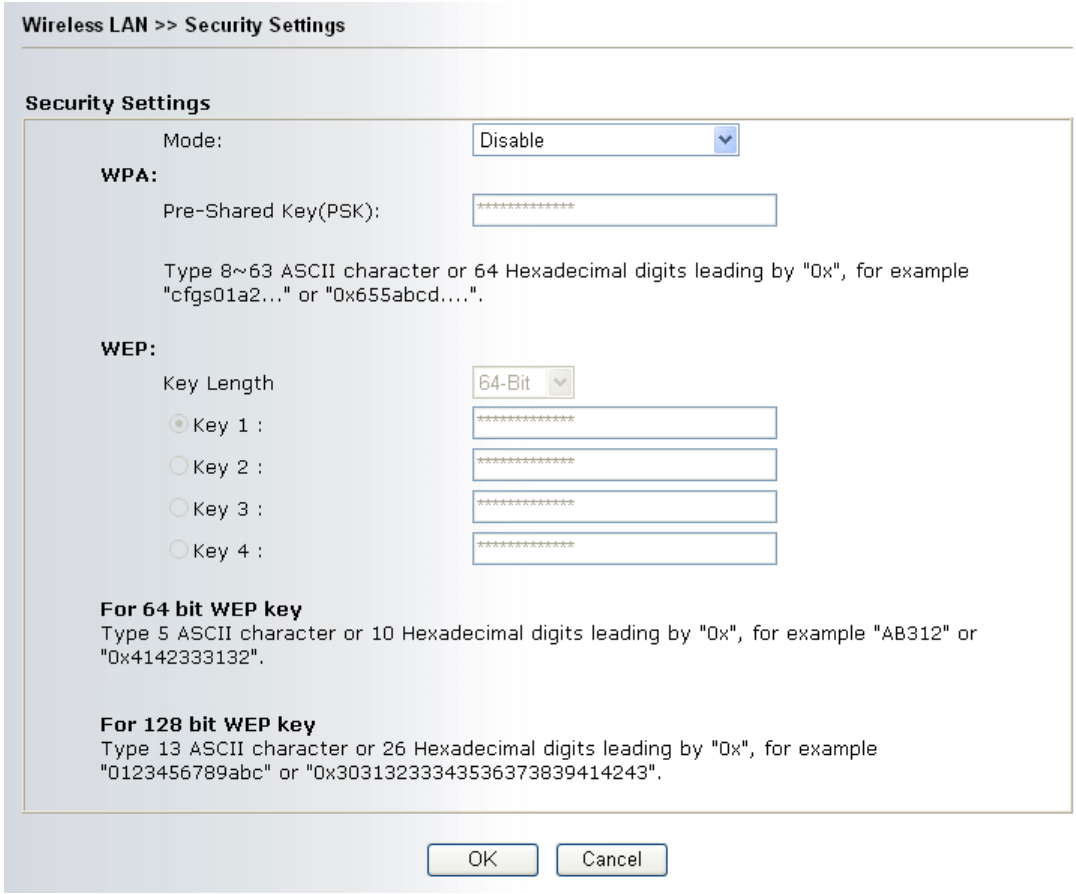
Mode Select an appropriate wireless mode.
Mixed (11b+11g)-The router communicates with standard 802.11b and standard 802.11g STAs simultaneously.
11g only-The router communicates with standard 802.11b STAs.
11b only-The router communicates with standard 802.11b STAs.



Scheduler	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Call Schedule** setup. The default setting of this filed is blank and the function will always work.
SSID and Channel	The default SSID is "default". We suggest you to change it. ***SSID***- Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. ***Channel***- Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while doing site survey
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network device only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

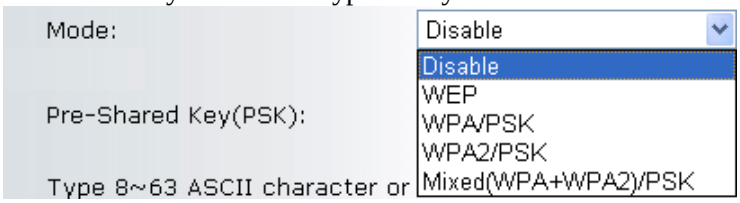
3.6.3 Security

This page allows you to set security with different modes. After configuring the correct settings, please click **OK** to save and invoke it.



Mode

Disable-Turn off the encryption mechanism. For the security of your router, please select any one of the encryption mode here.
WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.
WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.
WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.
Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.



WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

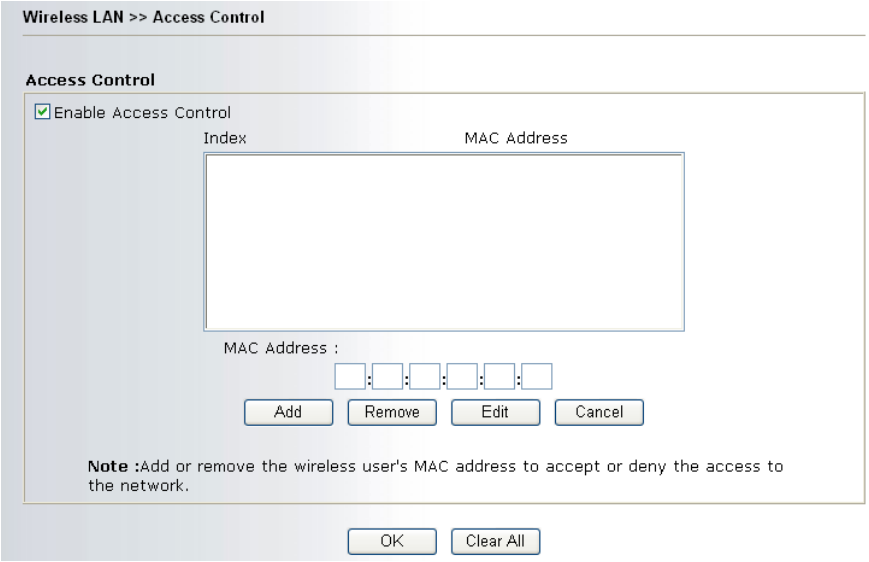
WEP

For key length 64 bits - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
For key length 128 bits - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM. (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D)

All wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.6.4 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right via the MAC address of wireless client. Only the valid MAC address that has been configured can access the wireless LAN. By clicking the **Access Control**, a new web page will appear as shown below. You could edit the clients' MAC addresses to control their access rights.



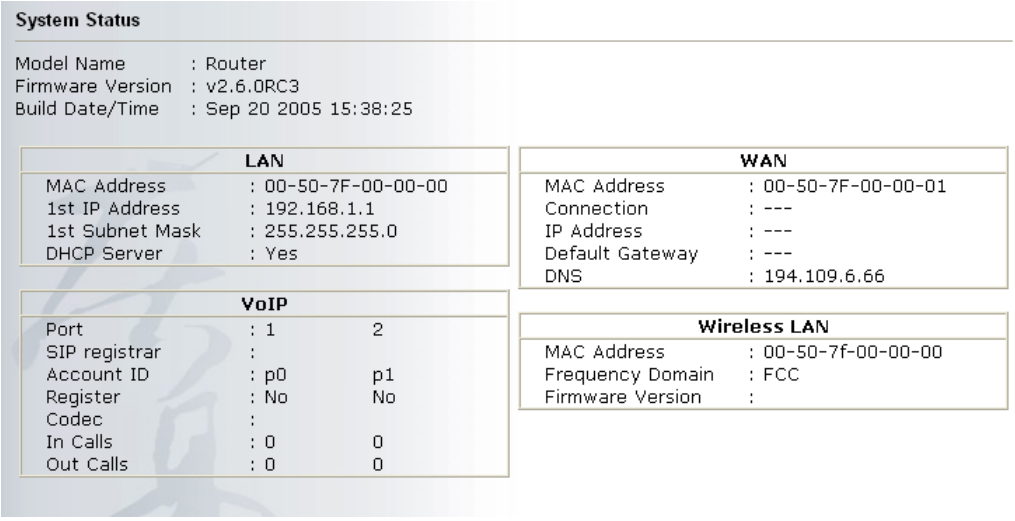
Enable Access Control	Select to enable the MAC Address access control feature.
Mac Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Remove	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

3.7 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

3.7.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.



Model Name Displays the model name of the router.

Firmware Version Displays the firmware version of the router.

Build Date&Time Displays the date and time of the current firmware build.

MAC Address Displays the MAC address of the LAN Interface.

1st IP Address Displays the IP address of the LAN interface.

1st Subnet Mask Displays the subnet mask address of the LAN interface.

DHCP Server Displays the current status of DHCP server of the LAN interface.

MAC Address Displays the MAC address of the WAN Interface.

IP Address Displays the IP address of the WAN interface.

Default Gateway Displays the assigned IP address of the default gateway.

DNS Displays the assigned IP address of the primary DNS.

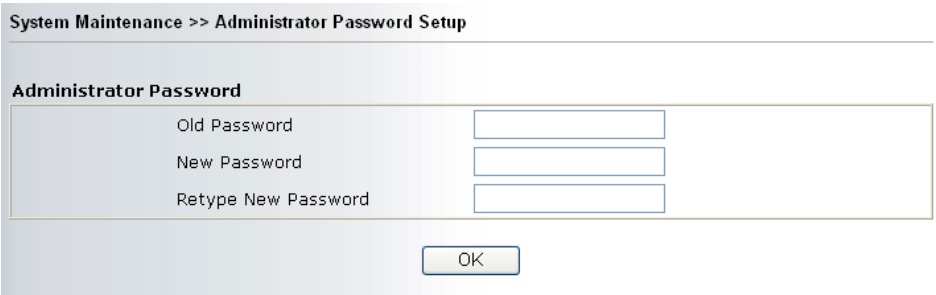
MAC Address Displays the MAC address of the wireless Interface.

Frequency Domain Displays the available channel supported by the wireless product. It varies in different country, Europe (13 usable channels), USA (11 usable channels).

Firmware Version Displays information about equipped WLAN card driver.

3.7.2 Administrator Password

This page allows you to set new password.



Old Password Type in the old password. The factory default setting for password is blank.

New Password Type in new password in this filed.

Retype New Password Type in the new password again.

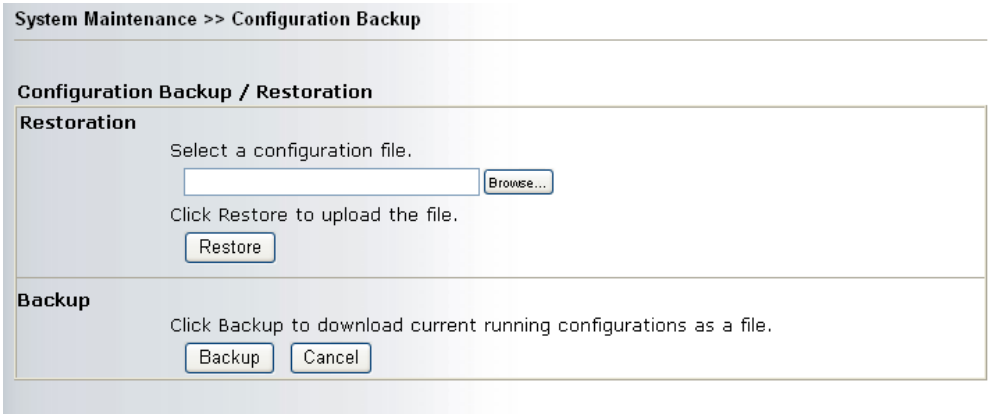
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

3.7.3 Configuration Backup

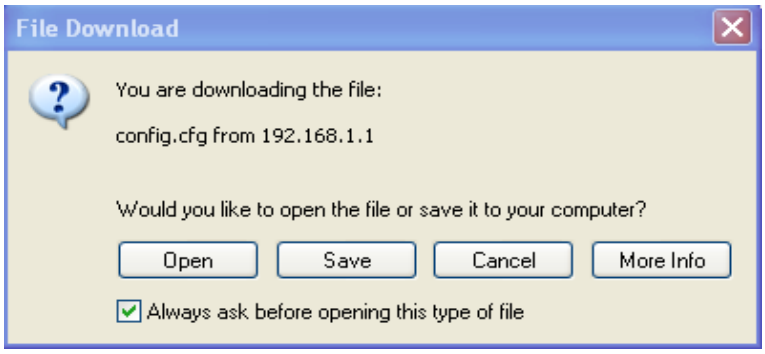
Backup the Configuration

Follow the steps below to backup your configuration.

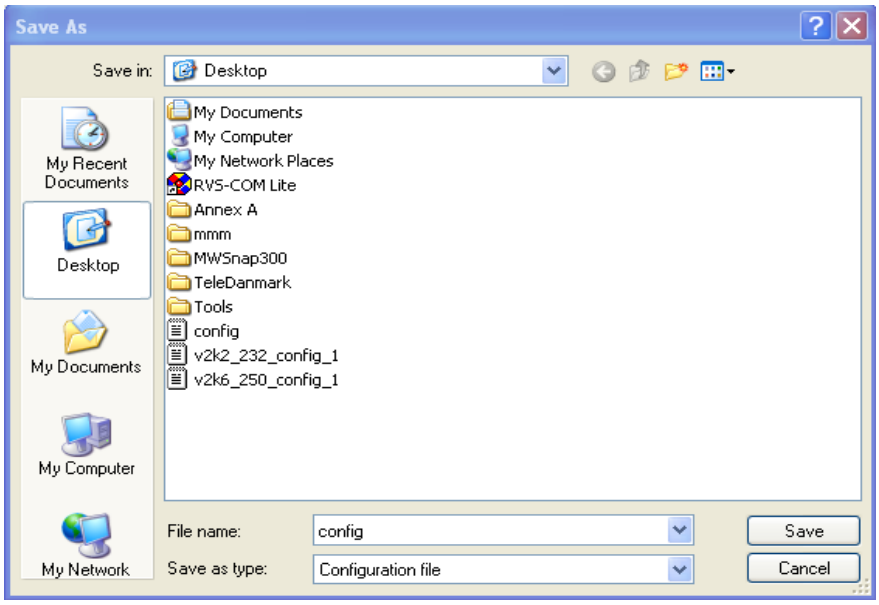
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.

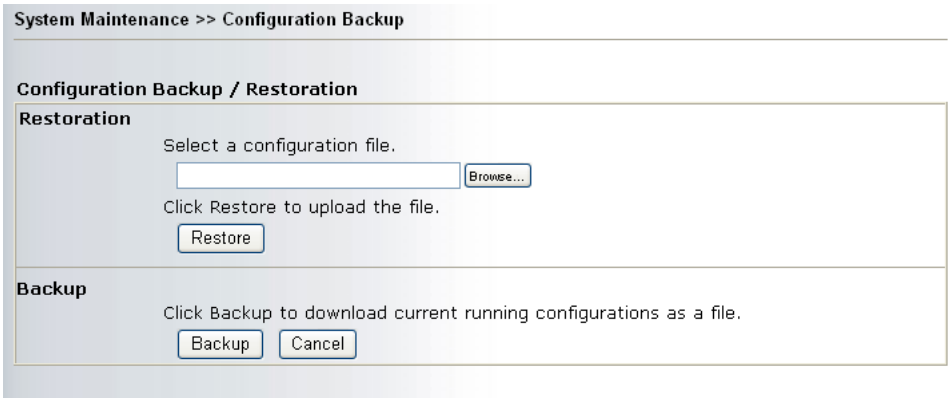


4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Restore Configuration

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

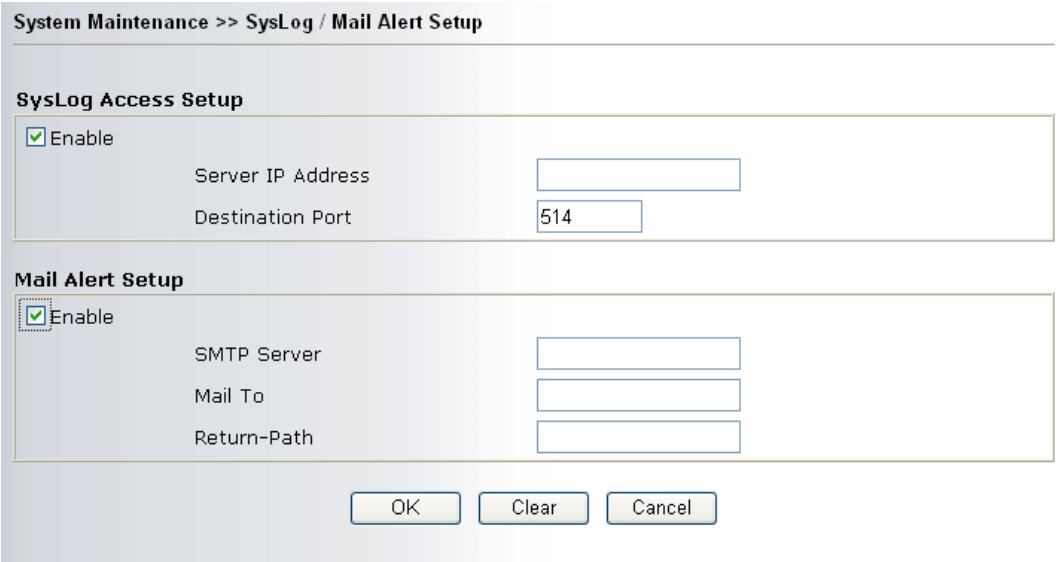


2. Click **Browse** button to choose the correct configuration file for uploading to the router.

3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

3.7.4 Syslog/Mail Alert

SysLog function is provided to help users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

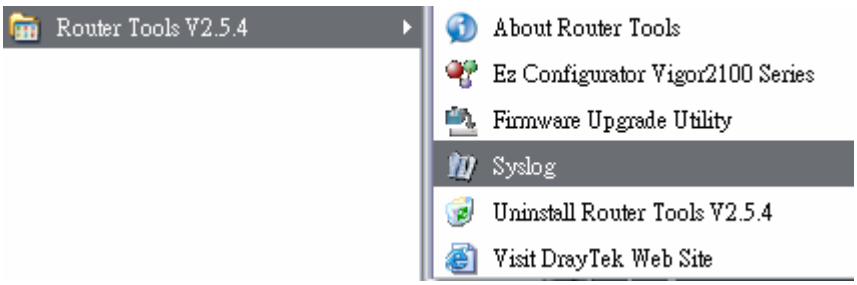


Enable	Click "**Enable**" to activate this function.
Syslog Server IP	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign a path for receiving the mail from outside.

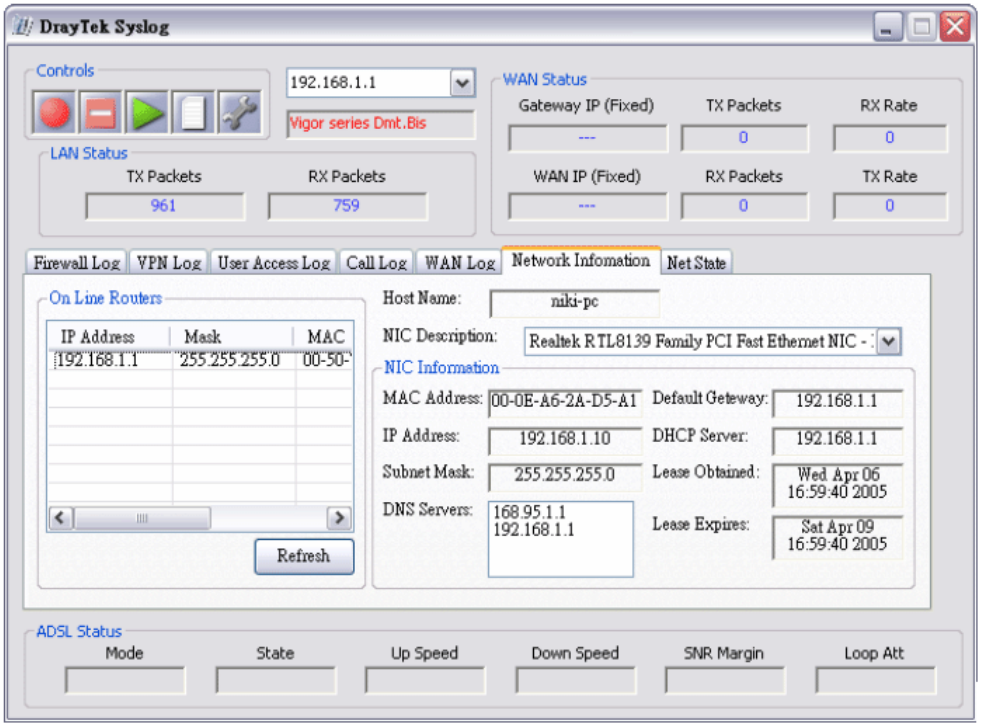
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.

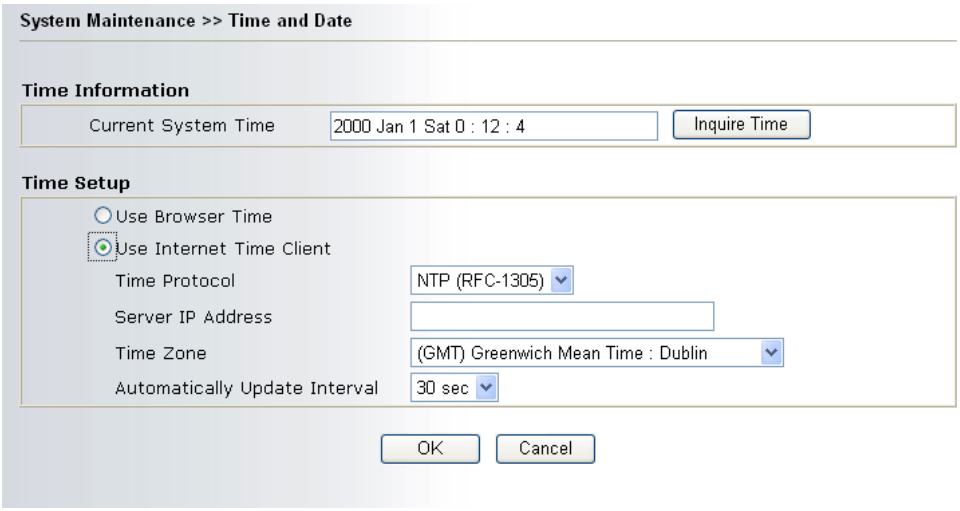


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



3.7.5 Time and Date

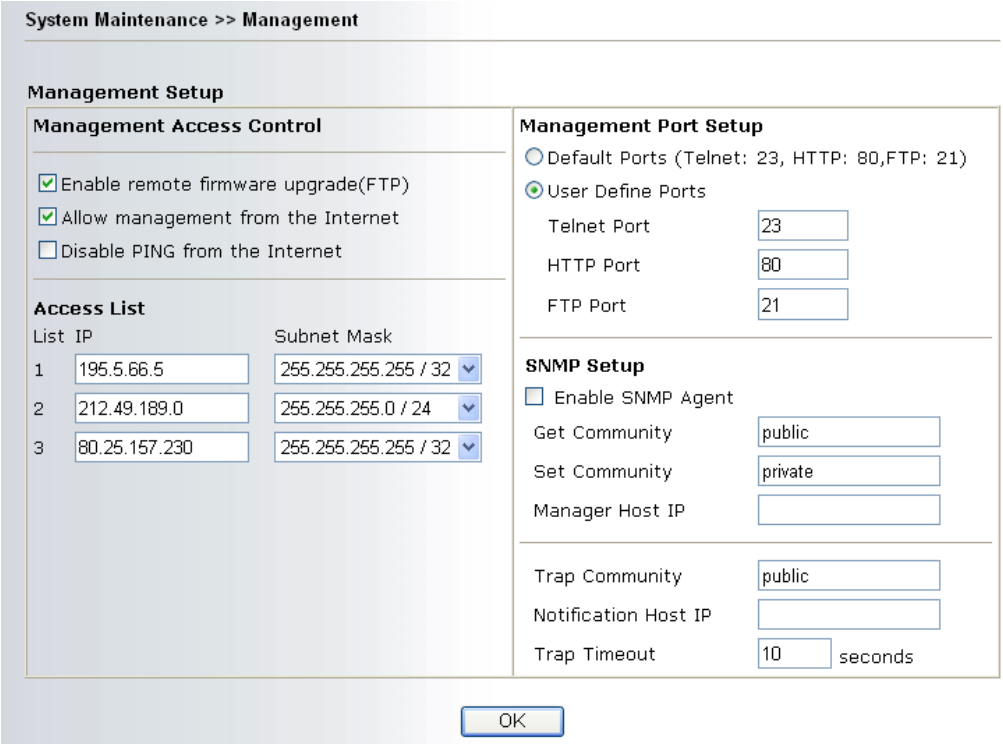
It allows you to specify where the time of the router should be inquired from.



Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time Client	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Protocol	Select a time protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the router is located.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.7.6 Management

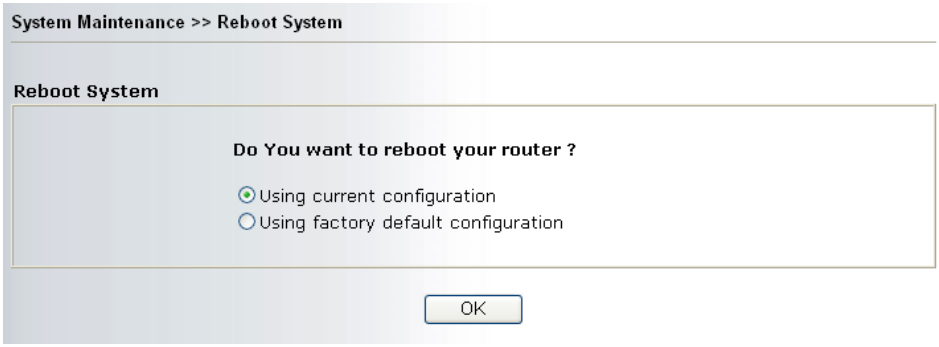


Enable remote firmware upgrade	Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).
Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **List IP** - Indicate an IP address allowed to login to the router. **Subnet Mask** - Represent a subnet mask allowed to login to the router.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet and HTTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.**
Set Community	Set community by typing a proper name. The default setting is **private.**
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.

Trap Community	Set trap community by typing a proper name. The default setting is **public.**
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

3.7.7 Reboot System

The Web Configurator may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.



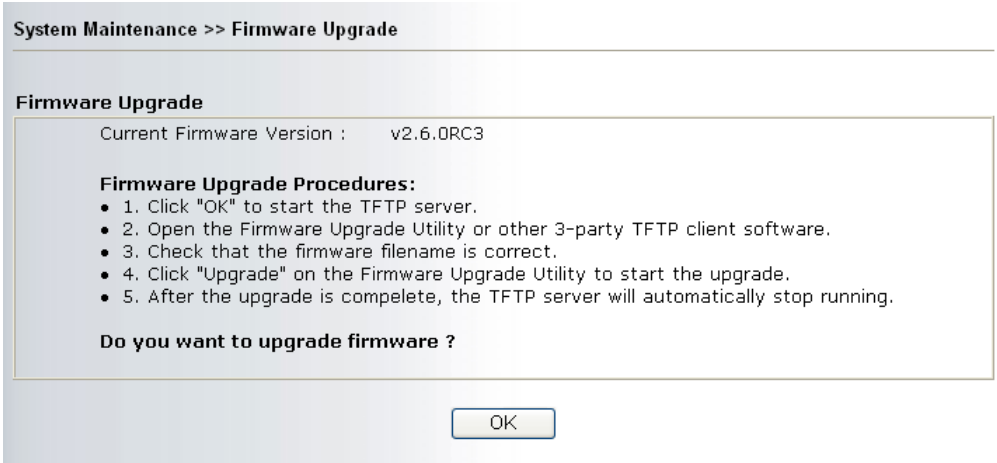
If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

3.7.8 Firmware Upgrade

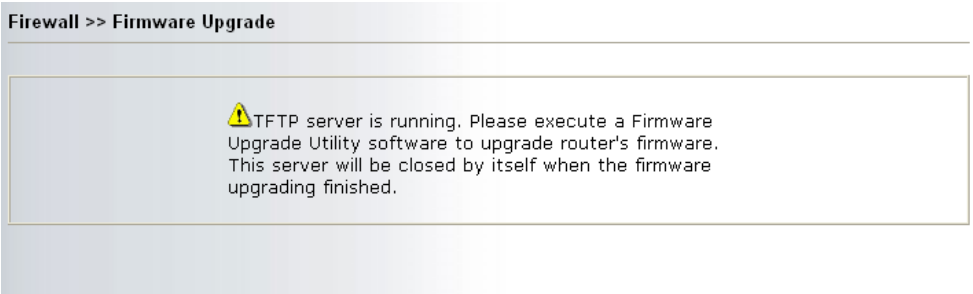
Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.



Click **OK**. The following screen will appear.



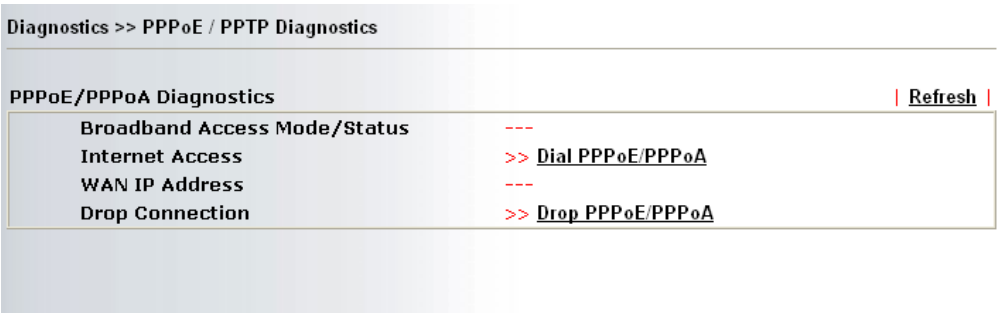
For the detailed information about firmware update, please go to Chapter 4.

3.8 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

3.8.1 PPPoE/PPPoA Diagnostics

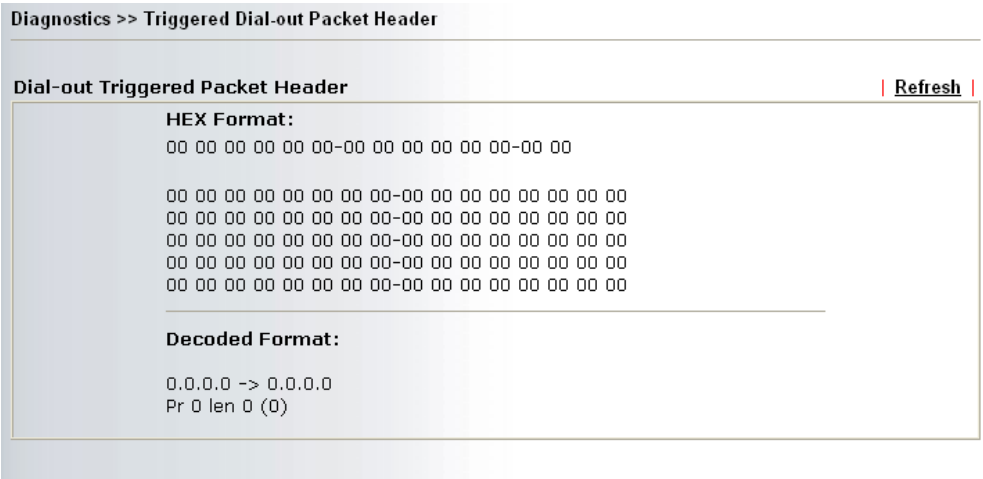
Click **Diagnostics** and click **PPPoE/PPPoA Diagnostics** to open the web page.



Refresh	To obtain the latest information, click here to reload the page.
Broadband Access Mode/Status	Display the broadband access mode and status. If the broadband connection is active, it will show Internet access mode is enabled. If the connection is idle, it will show "---".
WAN IP Address	The WAN IP address for the active connection.
Dial PPPoE or PPPoA	Click it to force the router to establish a PPPoE or PPPoA connection.

3.8.2 Triggerred Dial-out Packet Header

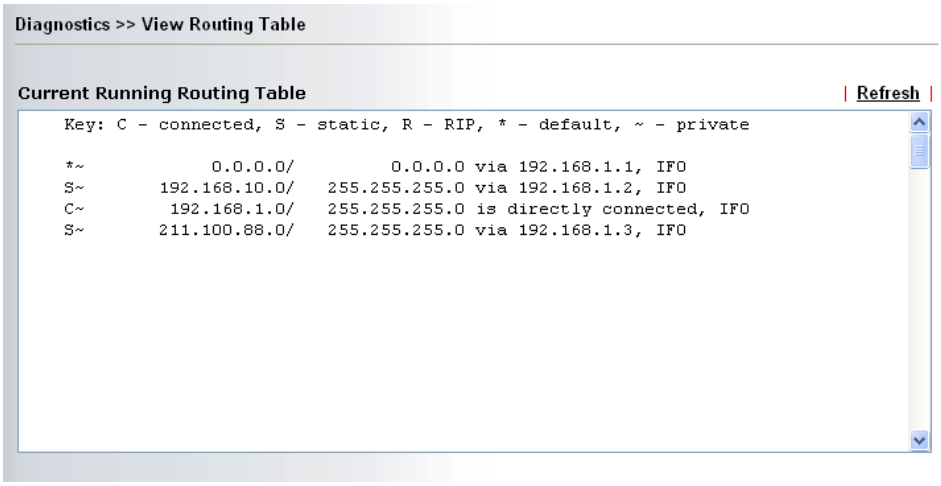
Click **Diagnostics** and click **Dial-out Trigger** to open the web page.



Refresh	Click it to reload the page.

3.8.3 Routing Table

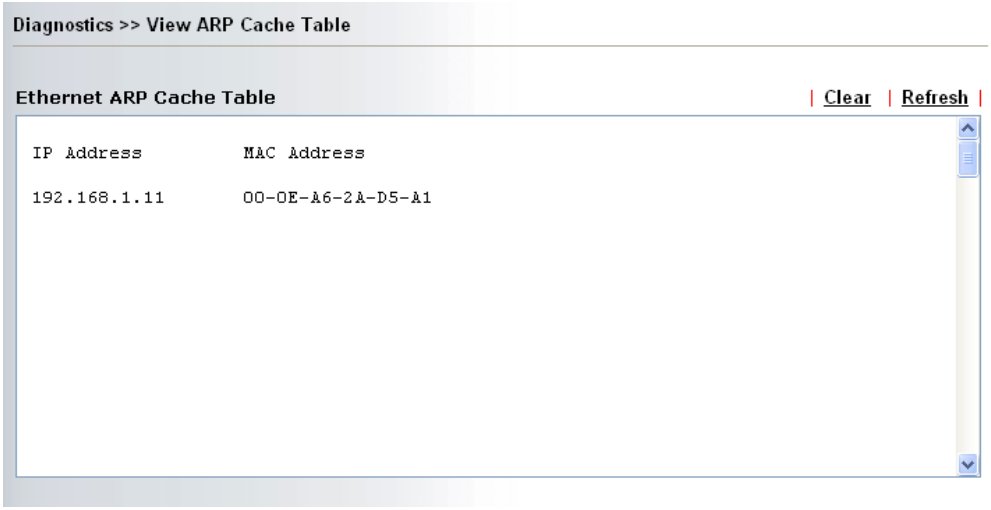
Click **Diagnostics** and click **Routing Table** to open the web page.



Refresh Click it to reload the page.

3.8.4 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



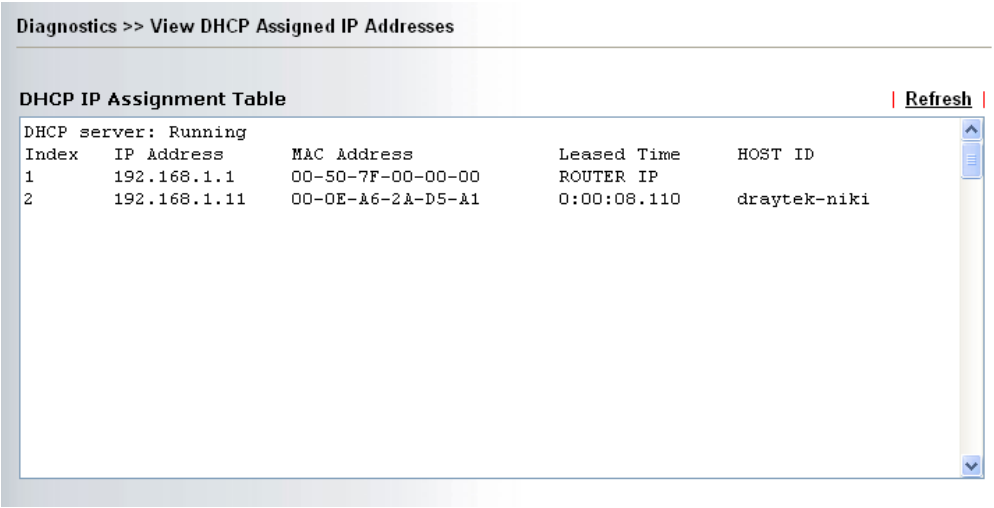
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

3.8.5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

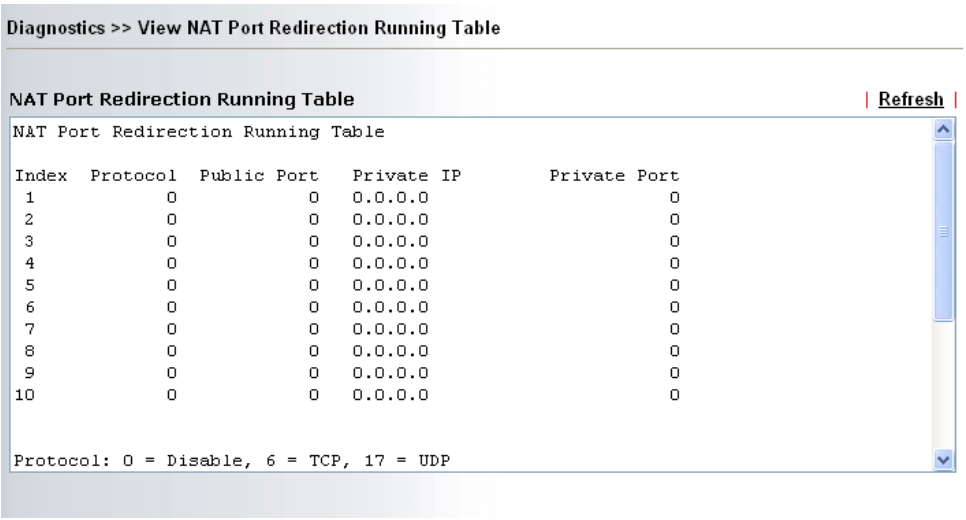
Click **Diagnostics** and click **DHCP Table** to open the web page.



Refresh Click it to reload the page.

3.8.6 NAT Port Redirection Table

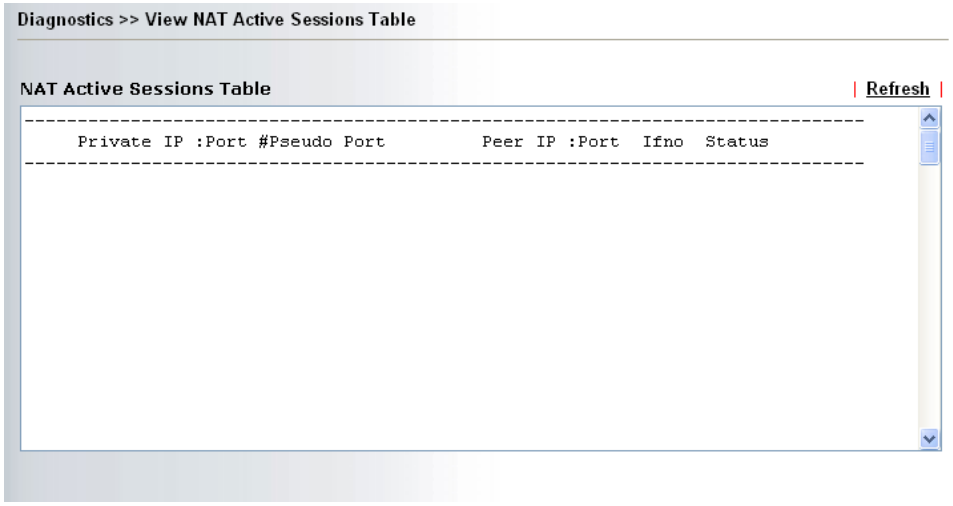
Click **Diagnostics** and click **NAT Port Redirection Table** to open the setup page.



Refresh Click it to reload the page.

3.8.6 NAT Active Sessions Table

Click **Diagnostics** and click **NAT Active Sessions Table** to open the setup page.

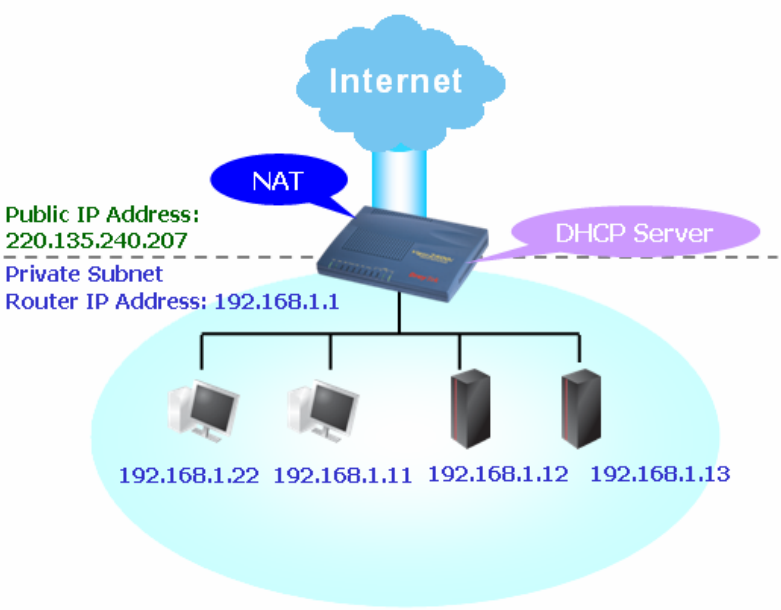


Refresh Click it to reload the page.

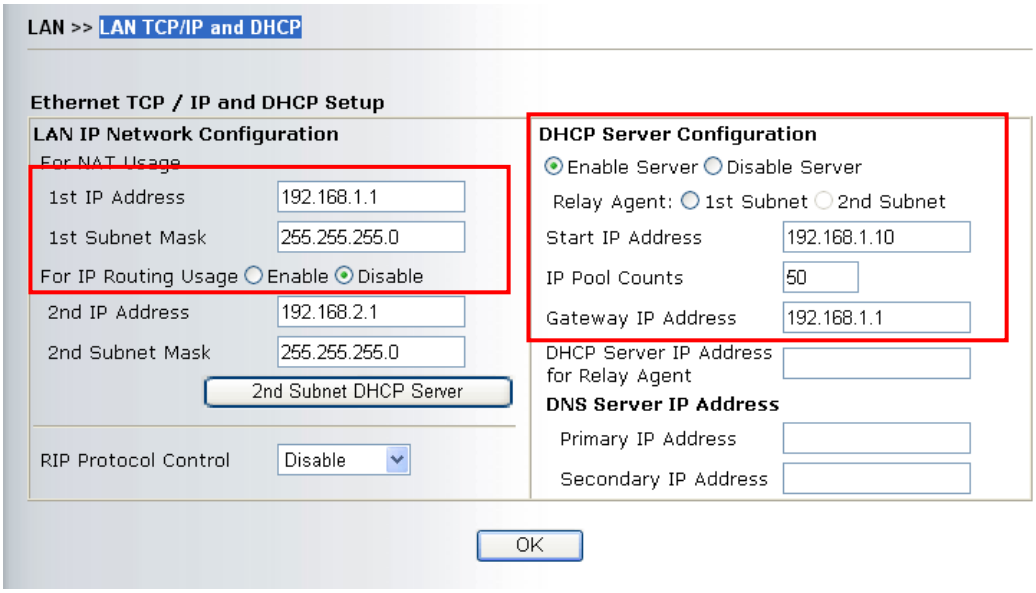
4 Application and Examples

4.4 LAN – Created by Using NAT

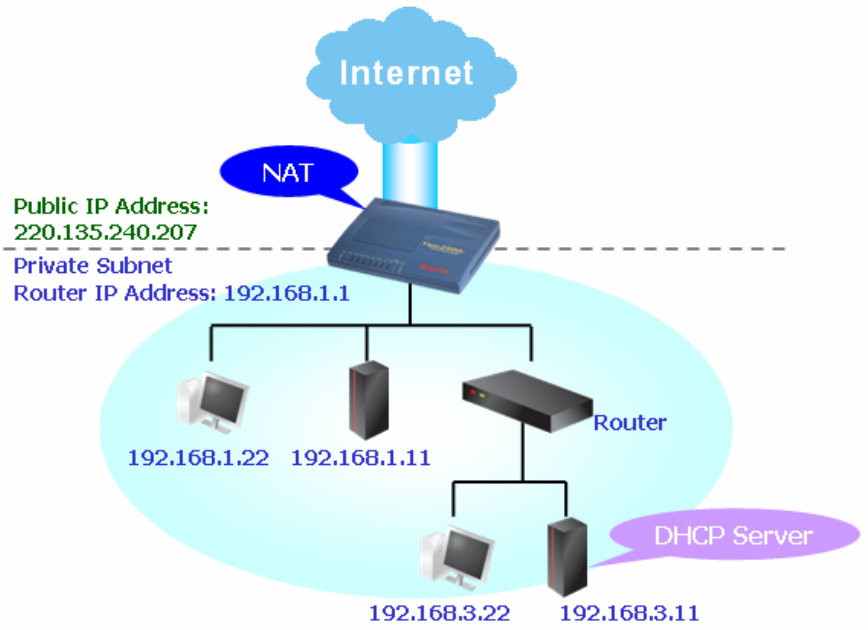
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



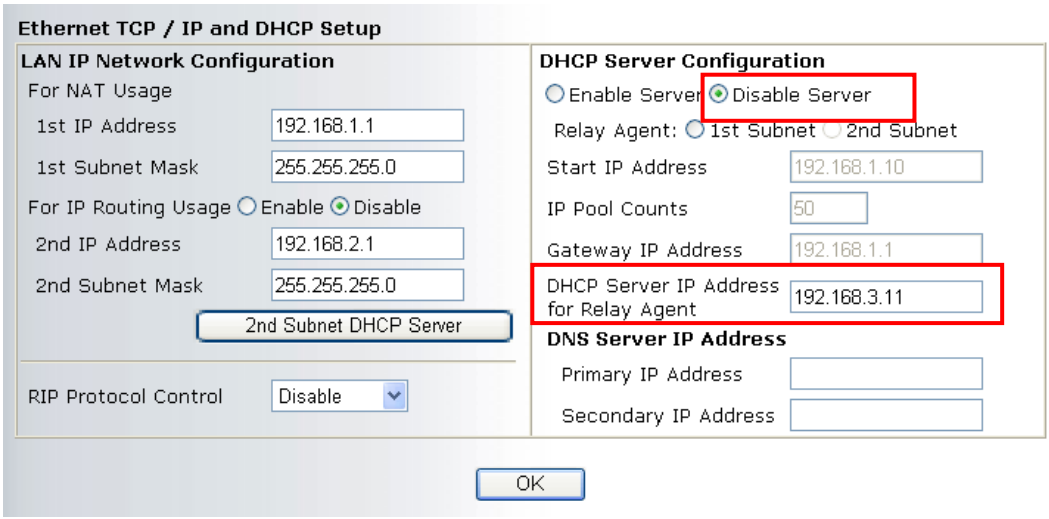
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.



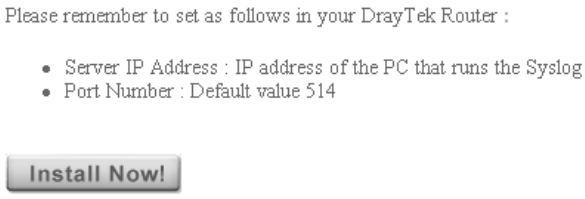
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



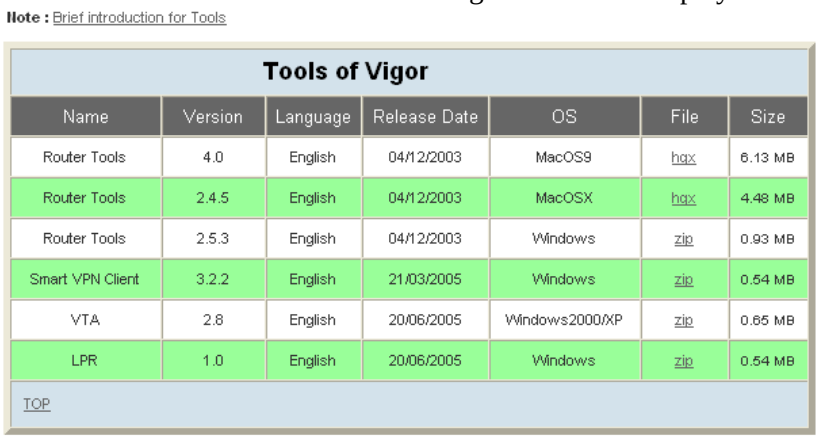
4.2 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

1. Insert CD of the router to your CD ROM.
2. From the webpage, please find out **Utility** menu and click it.
3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.

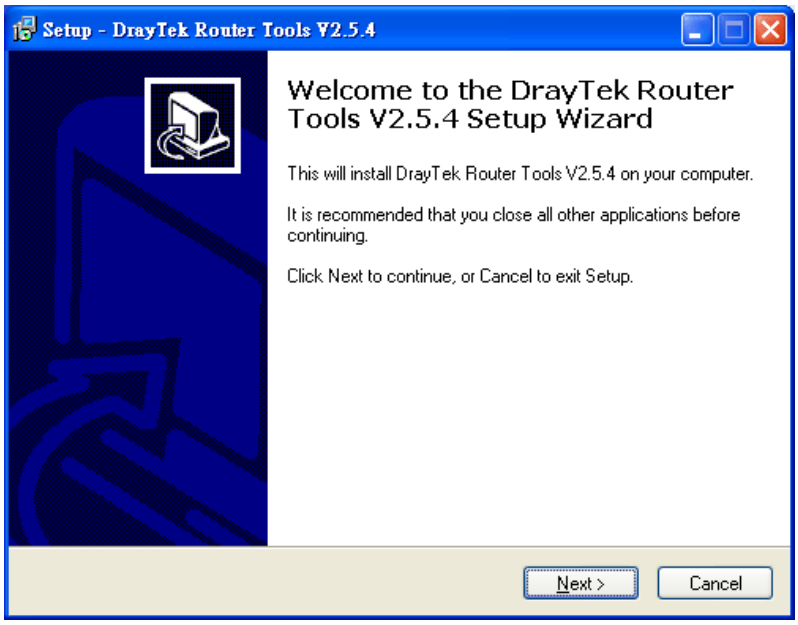


4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
5. Go to **www.draytek.com** to find out the newly update firmware for your router.
6. Access into **Support Center** >> **Downloads**. Find out the model name of the router and click the firmware link. The Tools of Vigor router will display as shown below.

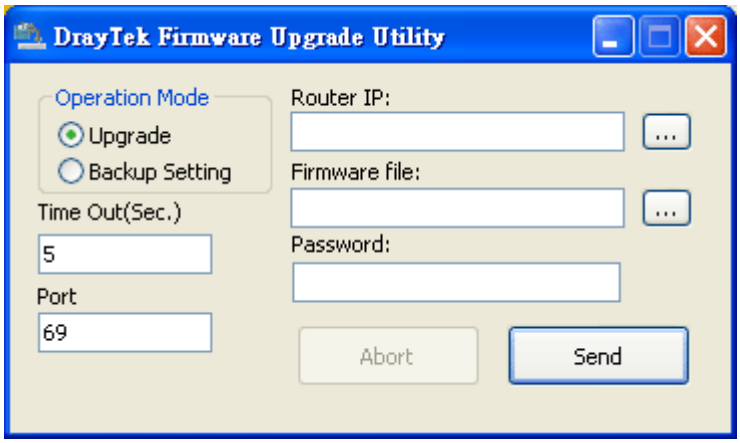


7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
8. Next, decompress the zip file.

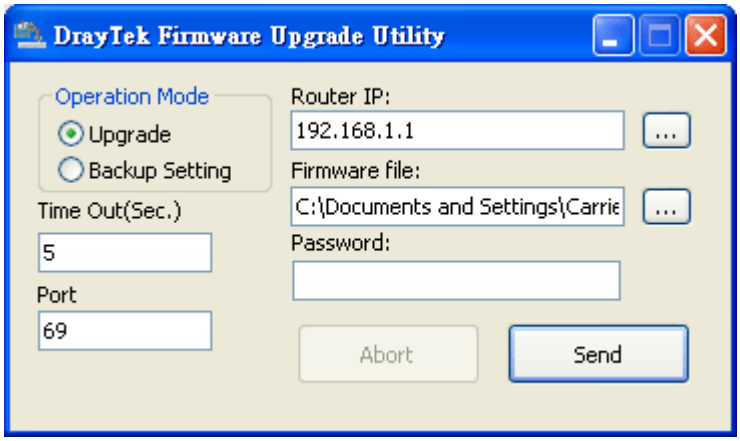
9. Double click on the icon of router tool. The setup wizard will appear.



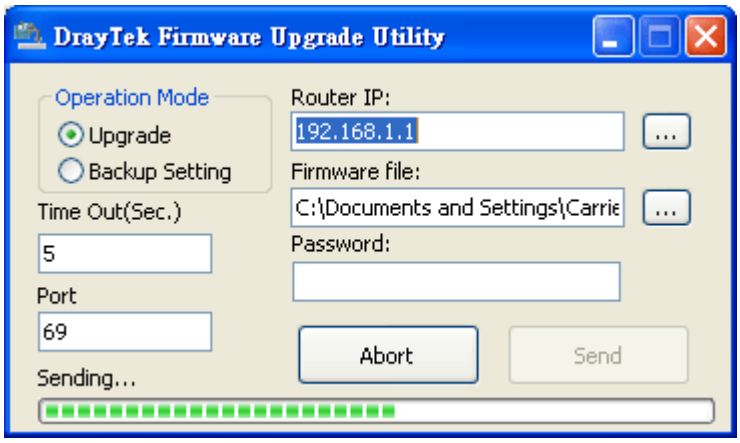
10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
11. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.



12. Type in your router IP, usually **192.168.1.1**.
13. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.



14. Click **Send**.



15. Now the firmware update is finished.

5 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

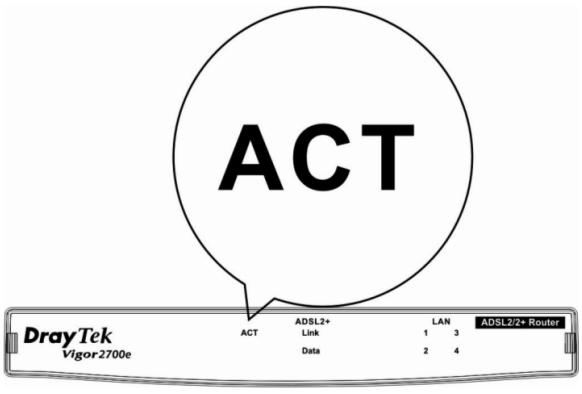
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

4.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**2.1 Hardware Installation"** for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"2.1 Hardware Installation"** to execute the hardware installation again. And then, try again.

4.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

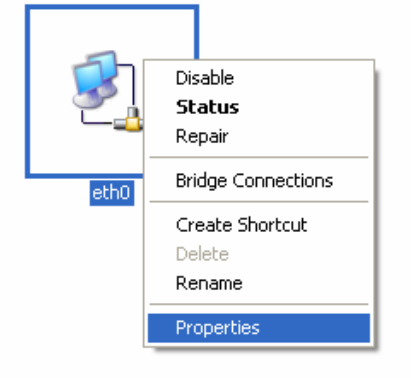
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

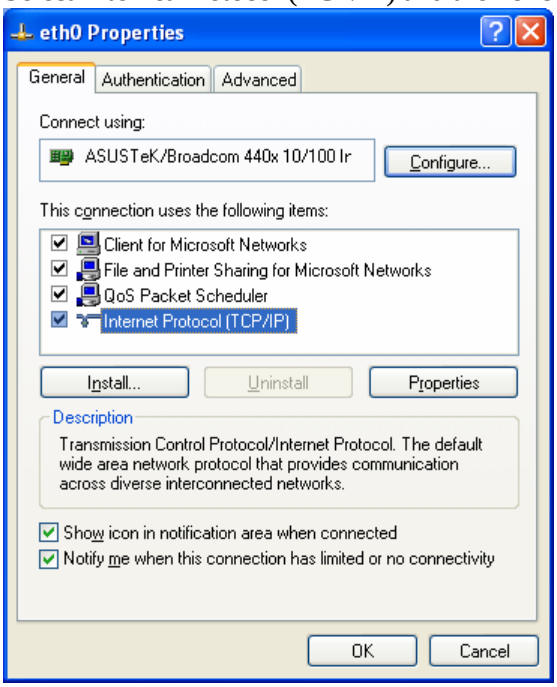
The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Go to Control Panel and then double-click on Network Connections.

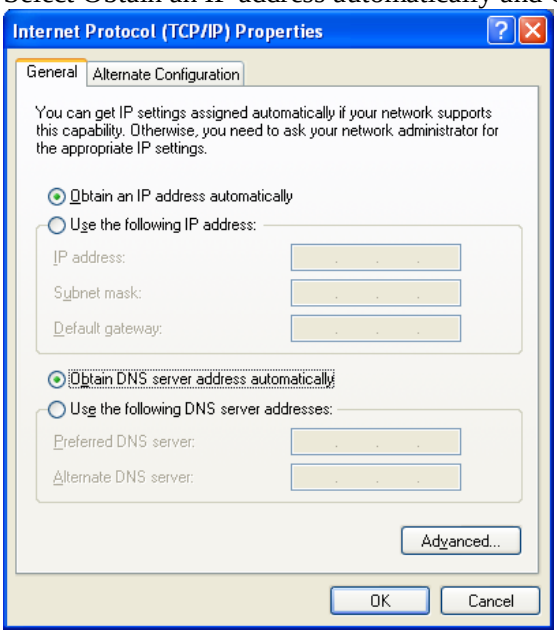
2. Right-click on Local Area Connection and click on Properties.



3. Select Internet Protocol (TCP/IP) and then click Properties.

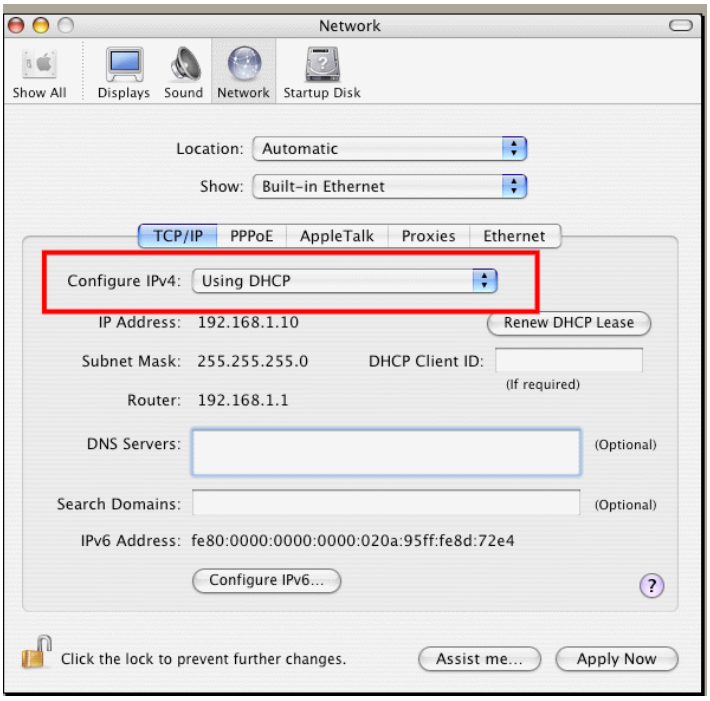


4. Select Obtain an IP address automatically and Obtain DNS server address automatically.



For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



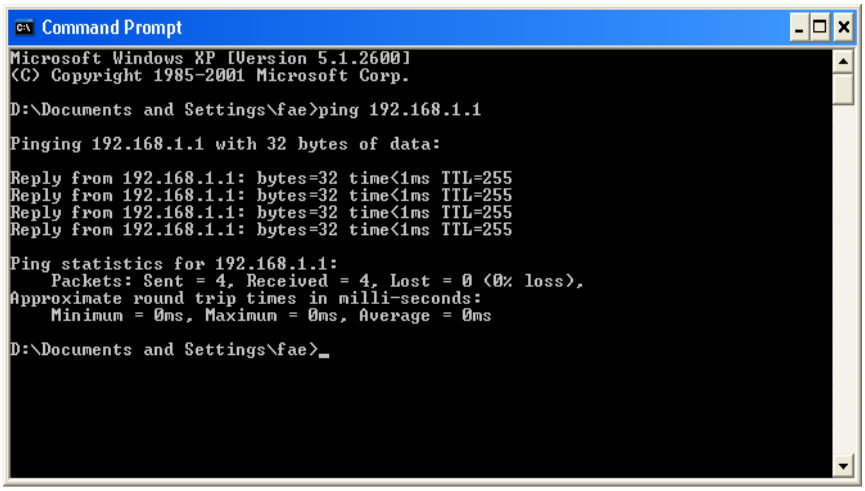
4.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 4.2)

Please follow the steps below to ping the router correctly.

For Windows

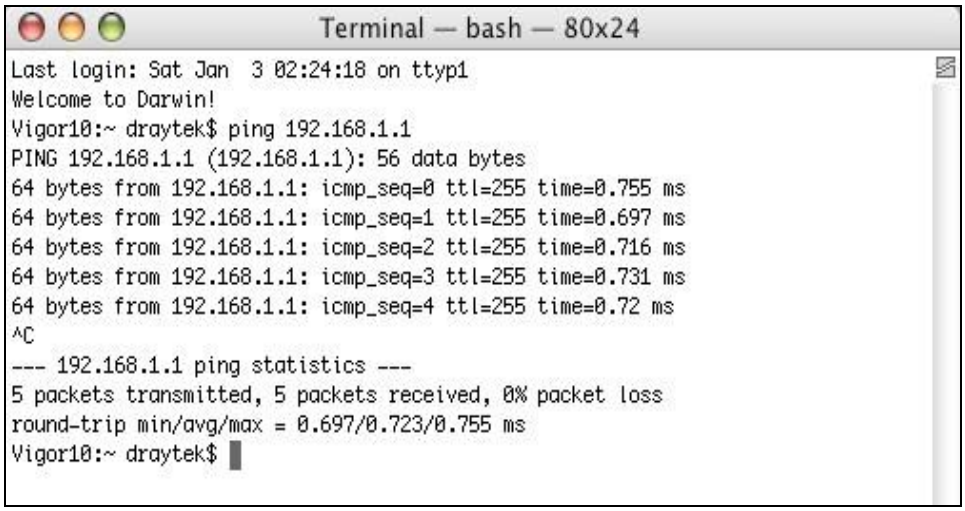
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



3. Type ping 192.168.1.1 and press [Enter]. It the link is OK, the line of "Reply from 192.168.1.1: bytes=32 time<1ms TTL=25" will appear.
4. If the line does not appear, please check the IP address setting of your computer.

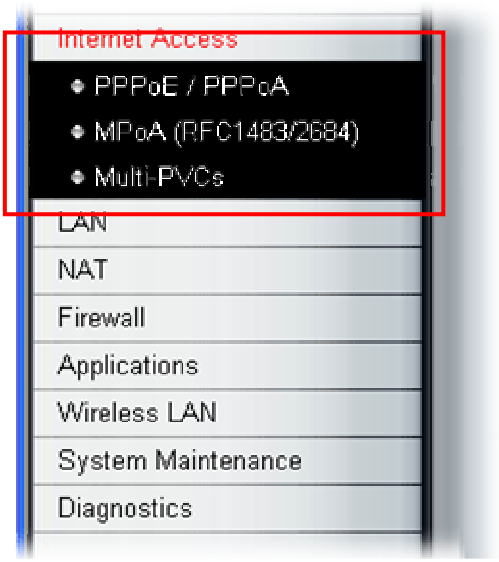
For MacOs (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. It the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

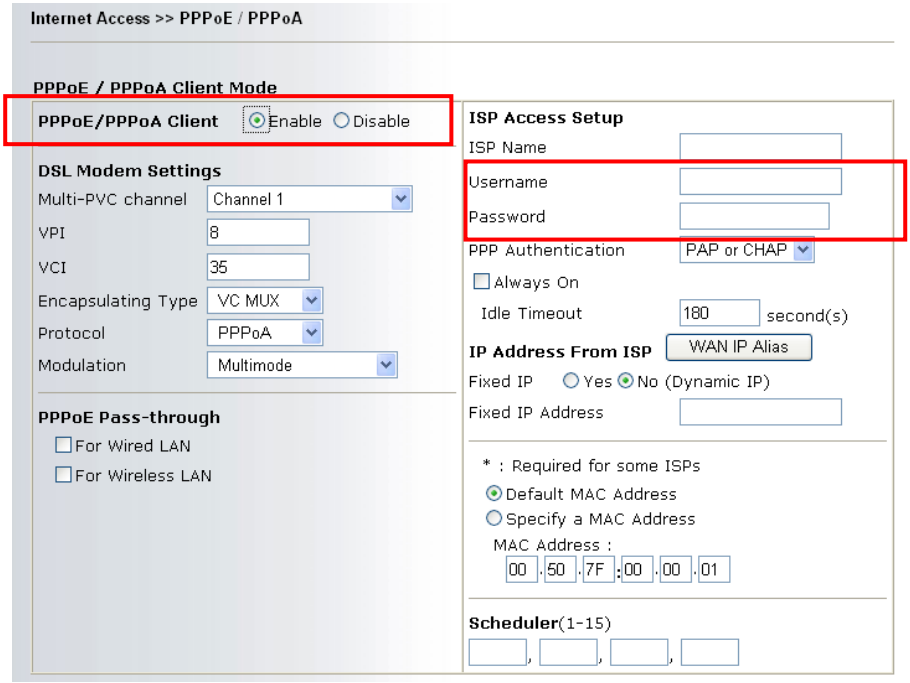
4.4 Checking If the ISP Settings are OK or Not

Click **Internet Access** group and then check whether the ISP settings are set correctly.



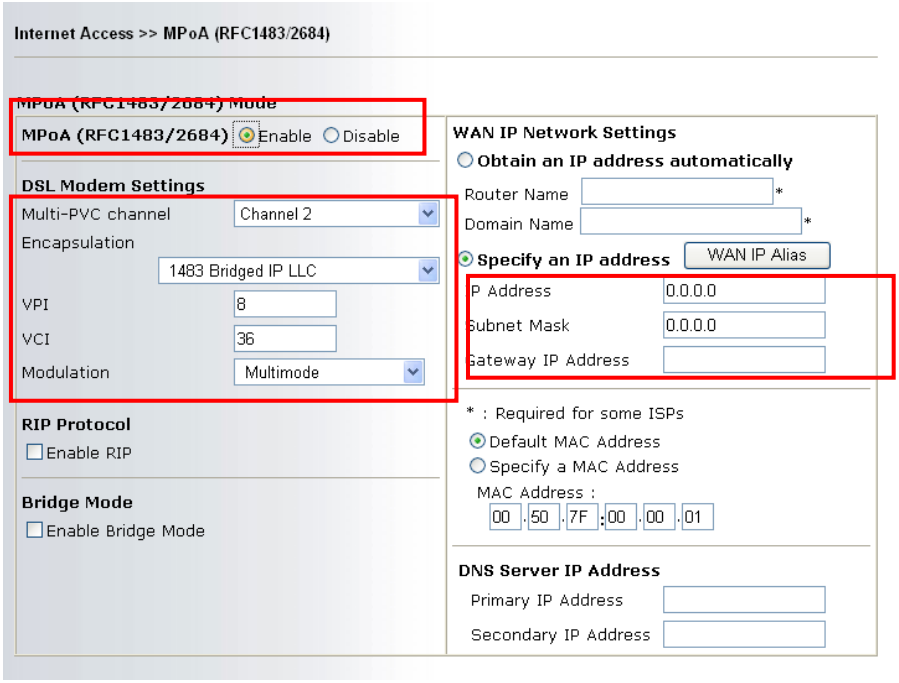
For PPPoE/PPPoA Users

1. Check if the **Enable** option is selected.
2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.



For MPoA Users

1. Check if the **Enable** option for Broadband Access is selected.



2. Check if all parameters of **DSL Modem Settings** are entered with correct value that provided by your ISP. Especially, check if the encapsulation is selected properly or not (it should be the same with the setting on **Quick Start Wizard**).

3. Check if **IP Address, Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

4.5 Backing to Factory Default Setting If Necessary

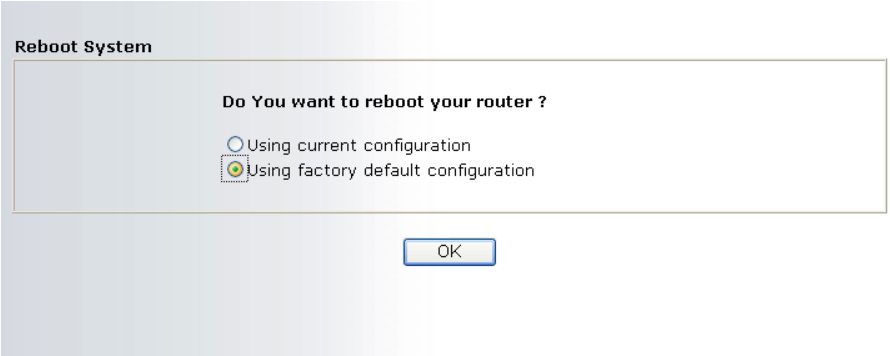
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

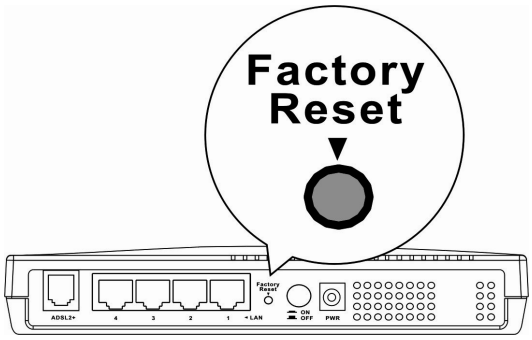
You can reset the router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the router will return all the settings to the factory settings.



Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

4.6 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.